FEREC520/720
取扱説明書

株式会社ネットスプリング
2014 年 10 月

はじめに

　このたびは Netspring FEREC520/720 をお買い上げ頂き、誠にありがとうございます。正しく安全にお使い頂くため、ご使用前に必ず本書をお読みください。

　本書は、FEREC Ver 2.4.7 を対象にしています。

安全上の注意

　次の表示区分は、表示内容を守らず、誤った使用をした場合に生じる危険や損害の程度を説明しています。

	警告	この表示は、誤った使用をした場合、「人が死亡または重傷を負う可能性が想定される」内容を示しています。
	注意	この表示は、誤った使用をした場合、「人が障害を負う可能性または物的損害が発生する可能性が想定される」内容を示しています。

　次の表示区分は、お守りいただく内容を説明しています。

	禁止（してはいけないこと）を示しています。
	強制（必ず実行していただくこと）を示しています。

	警告	
	同梱の電源ケーブル、AC アダプタ（FEREC520 のみ）以外は、使用しないでください。	故障したり、過熱、発煙するおそれがあり、火災、感電の原因となります。
	強い衝撃を与えたり、投げつけたりしないでください。	故障したり、過熱、発煙するおそれがあり、火災、感電の原因となります。

	分解、改造をしないでください。	火災、感電、ケガなどの事故または故障の原因となります。
	水につけたり、ぬらしたりしないでください。	故障したり、過熱、発煙するおそれがあり、火災、感電の原因となります。
	ぬれた手で本製品やACアダプタ、プラグを触らないでください。	火災、感電、ケガなどの事故または故障の原因となります。
	本製品に水や殺虫剤などをかけたりしないでください。	故障したり、過熱、発煙するおそれがあり、火災、感電の原因となります。
	端子部を触らないでください。	故障したり、感電、ケガのおそれがあります。
	通気孔をふさがないでください。	故障したり、過熱、発煙するおそれがあり、火災、感電の原因となります。
	通気孔に物を差し込まないでください。	故障したり、過熱、発煙するおそれがあり、火災、感電の原因となります。
	本体または AC アダプタが異常に熱くなったり、煙が出たり、変なにおいがした場合は、電源プラグをコンセントから抜いて弊社サポートセンターへご連絡ください。	火災の原因となります。

	注意	
	本書に記載されていない操作はしないでください。	故障の原因となります。
	動作中に本体を長時間触らないでください。	低温やけどを負う可能性があります。

諸注意

- 本製品は「外国為替および外国貿易管理法」に定められる戦略物資等に該当します。本製品を輸出または日本国外へ持ち出す際には、事前に弊社の書面による承諾を得ることのほか、同法および関連の法令に基づく手続きが必要です。
- 本製品は日本国内仕様のため、修理・保守サービス・技術サポートなどの対応は、日本国外ではお受けできませんのでご了承ください。
- 日本国外ではその国の法律または規制により、本製品を使用できないことがあります。このような国では、本製品を使用した結果罰せられることがありますが、弊社は一切の責任を負いかねますのでご了承ください。

商標

- FEREC は株式会社ネットスプリングの登録商標です。
- 本書に記載されている他社製品名は、一般に各社の商標または登録商標です。

本書について

- 本書の著作権は株式会社ネットスプリングに帰属します。本書の一部または全部を無断で転載、複製、改変などを行うことは禁じられています。
- 本書の校正には細心の注意を払っておりますが、技術的な誤りまたは誤植のある可能性があります。お気付きの点がございましたら、弊社までご連絡ください。
- 本書に記載された内容は、予告なく改良または変更する場合があります。

改訂番号	14
改訂日	2014 年 10 月 27 日

目次

1. お使いいただく前に

1.1. 製品の特徴

ウェブブラウザ認証

端末の OS や環境に依存することがなく利用できるウェブブラウザによる認証方式です。

認証ページ強制表示

利用者がウェブブラウザを起動すると、FEREC の認証ページが強制的に表示されます。

カスタムページ機能

認証ページには、カスタムページ機能フレームがあり、ポータルサイトとして利用できます。

ブリッジ/NAT 選択切替

ブリッジモード・NAT モード切替でどんなネットワークにもスムーズに対応できます。

多様な認証方式

内部認証、RADIUS 認証、LDAP 認証など多様な認証方式に対応しています。

便利な内部認証機能

管理ページで簡単にアカウント発行や削除を行うことができます。

利用禁止アカウント設定

不正利用者を切断して、応急措置が可能です。

アクセスコントロール

きめ細かくユーザ毎にアクセスを制限します。

簡易な設定・運用管理

ウェブブラウザによる簡易な設定、運用管理ができます。

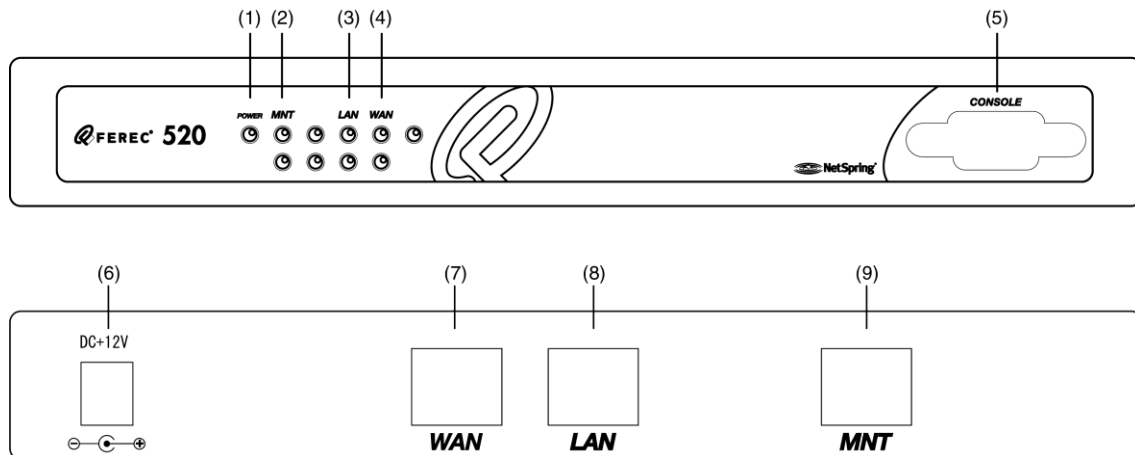
利用状況・ログ管理

ユーザ利用状況をリアルタイム表示します。また syslog により利用履歴の管理も可能です。

最新ファームウェアを提供

最新ファームウェアは FEREC オフィシャルサイト（http://www.ferec.jp/）からダウンロードできます。

1.2. 本体各部の名称

FEREC520(FAJ520)の各部の名称と機能は以下のとおりです。

(1) POWER LED
電源が ON の時に点灯します。

(2) MNT LED

(3) LAN LED

(4) WAN LED
WAN, LAN, MNT ポートのインジケータです。上段は各ポートが100Mbps(FastEthernet)でリンクアップすれば点灯し、10Mbps でリンクアップした場合は消灯します。下段は各ポートにアクセスがあれば点滅します。

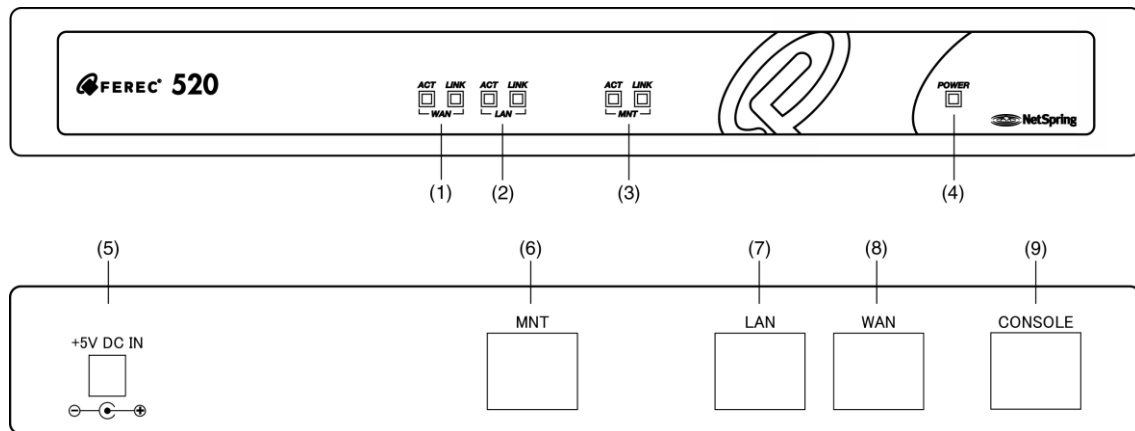
(5) CONSOLE ポート
シリアルコンソール用の RS-232C ポートです。PC と接続する際はクロスケーブルを使用します。

(6) DC 入力
電源コネクタです。必ず FAJ520 付属の AC アダプタを接続してください。

(7) WAN ポート

(8) LAN ポート

(9) MNT ポート
WAN, LAN, MNT のイーサネットポートです。

FEREC520(FAJ521)の各部の名称と機能は以下のとおりです。

(1) WAN LED

(2) LAN LED

(3) MNT LED

WAN, LAN, MNT ポートのインジケータです。右側は各ポートがリンクアップすれば橙色に点灯します。左側は各ポートにアクセスがあれば緑色に点滅します。

(4) POWER LED

電源が ON の時に点灯します。

(5) DC 入力

電源コネクタです。必ず FAJ521 付属の AC アダプタを接続してください。

(6) MNT ポート

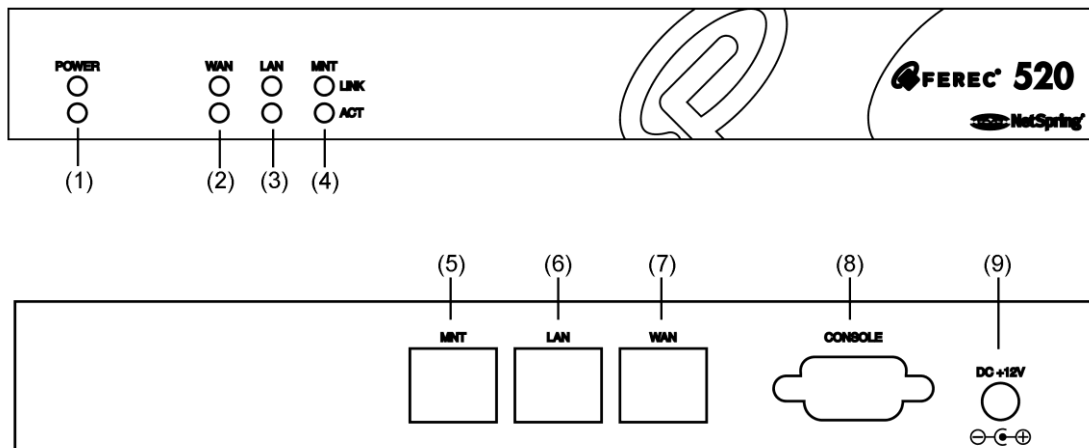
(7) LAN ポート

(8) WAN ポート

WAN, LAN, MNT のイーサネットポートです。

(9) CONSOLE ポート

シリアルコンソール用の RJ45 ポートです。

FEREC520(FAJ522)の各部の名称と機能は以下のとおりです。

(1) POWER LED

上側は電源が ON の時に点灯します。

(2) WAN LED

(3) LAN LED

(4) MNT LED

WAN, LAN, MNT ポートのインジケータです。上側は各ポートがリンクアップすれば緑色に点灯します。下側は各ポートにアクセスがあれば橙色に点滅します。

(5) MNT ポート

(6) LAN ポート

(7) WAN ポート

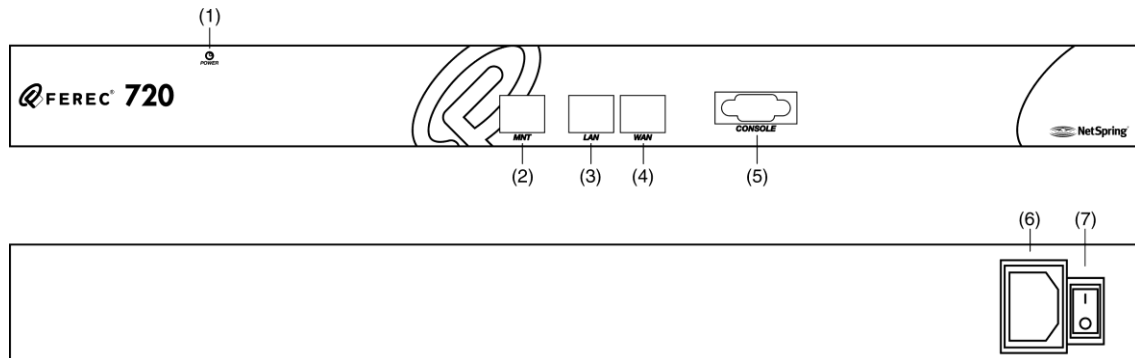
WAN, LAN, MNT のイーサネットポートです。

(8) CONSOLE ポート

シリアルコンソール用のポートです。PC と接続する際はクロスケーブルを使用します。

(9) DC 入力

電源コネクタです。必ず FAJ522 付属の AC アダプタを接続してください。

FEREC720(FBJ720)の各部の名称と機能は以下のとおりです。

(1) POWER LED

電源が ON の時に点灯します。

(2) WAN

(3) LAN

(4) MNT

WAN, LAN, MNT のイーサネットポートとインジケータです。各ポートの右上の LED はリンクアップすれば点灯します。1000Mbps（GbE）でリンクアップした場合は橙色に、100Mbps（FastEthernet）でリンクアップした場合は緑色に点灯します。10Mbps でリンクアップした場合 LED は消灯します。左上の LED はアクセスがあれば点滅します。各ポートは MDI/MDI-X を自動認識します。

(5) CONSOLE ポート

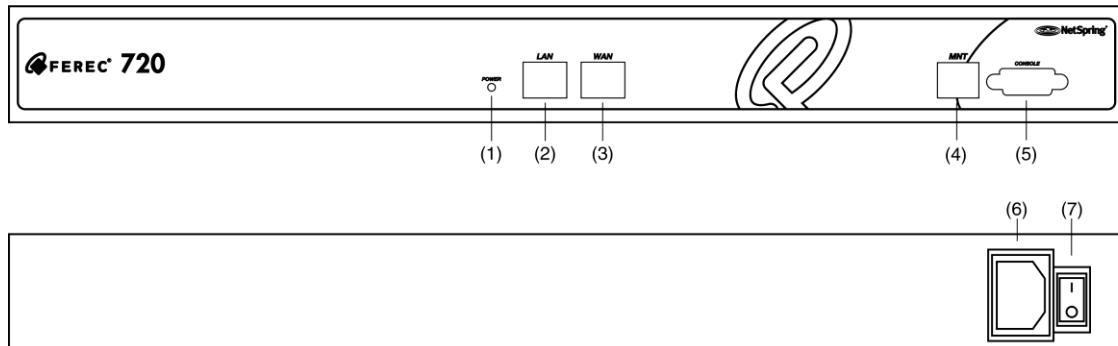
シリアルコンソール用の RS-232C ポートです。PC と接続する際はクロスケーブルを使用します。

(6) AC 入力

電源コネクタです。必ず付属の電源ケーブルを接続してください。

(7) 電源スイッチ

電源スイッチです。［○］側が OFF、［｜］側が ON です。

FEREC720(FBJ721)の各部の名称と機能は以下のとおりです。

(1) POWER LED

電源が ON の時に点灯します。

(2) LAN

(3) WAN

WAN, LAN のイーサネットポートとインジケータです。各ポートの右上の LED はリンクアップすれば黄色に点灯し、アクセスがあれば点滅します。

左上の LED は 1000Mbps(GbE)でリンクアップした場合は黄色に、100Mbps (FastEthernet)でリンクアップした場合は橙色に点灯します。10Mbps でリンクアップした場合は消灯します。各ポートは MDI/MDI-X を自動認識します。

(4) MNT

MNT のイーサネットポートとインジケータです。ポートの右上の LED はリンクアップすれば黄色に点灯し、アクセスがあれば点滅します。左上の LED は 100Mbps(FastEthernet)でリンクアップした場合は橙色に点灯し、10Mbps でリンクアップした場合は消灯します。

(5) CONSOLE ポート

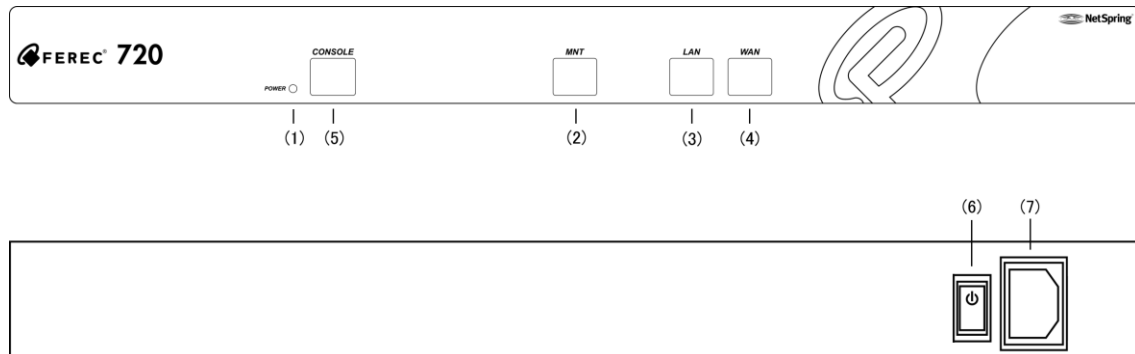
シリアルコンソール用の RS-232C ポートです。PC と接続する際はクロスケーブルを使用します。

(6) AC 入力

電源コネクタです。必ず付属の電源ケーブルを接続してください。

(7) 電源スイッチ

電源スイッチです。[○] 側が OFF、[｜] 側が ON です。

FEREC720(FBJ722)の各部の名称と機能は以下のとおりです。

(1) POWER LED

電源が ON の時に点灯します。

(2) MNT

(3) LAN

(4) WAN

WAN, LAN, MNT のイーサネットポートとインジケータです。各ポートの左上の LED はリンクアップすれば緑色に点灯し、アクセスがあれば点滅します。

右上の LED は 1000Mbps（GbE)でリンクアップした場合は緑色に、100Mbps (FastEthernet）でリンクアップした場合は橙色に点灯します。10Mbps でリンクアップした場合は消灯します。各ポートは MDI/MDI-X を自動認識します。

(5) CONSOLE ポート

シリアルコンソール用の RJ45 ポートです。

(6) 電源スイッチ

電源スイッチです。

(7) AC 入力

電源コネクタです。必ず付属の電源ケーブルを接続してください。

1.3.　起動・停止

FEREC520

- 起動する場合

  本体、AC アダプタ、電源ケーブルを接続します。

  30 秒程度で起動が完了し「ぷぴっ」というビープ音が鳴ります。

- 終了する場合

  終了する場合は AC アダプタ、電源ケーブルを抜きます。

FEREC720

- 起動する場合

  本体と電源ケーブルを接続し、電源スイッチを ON にします。

  30 秒程度で起動が完了し「ぷぴっ」というビープ音が鳴ります。

- 終了する場合

  終了する場合は電源スイッチを OFF にします。

NOTE

- 設定変更を行っている時は電源を切らないでください。

2. クライアント設定

2.1. クライアント端末のネットワーク設定上の注意点

FEREC を利用するクライアント端末のネットワーク設定を行う上での注意点は、以下の通りです。

2.1.1. ブリッジモード利用時

接続する LAN 上の規定通りに設定してください。FEREC を導入することにより、ネットワーク設定を変更する必要はありません。

2.1.2. NAT または NAPT モード利用時

クライアント端末のネットワーク設定は以下のようになります。

項目	注意点
IP アドレス	サーバから自動的に取得する（DHCP クライアント設定）
DNS サーバ	
デフォルトゲートウェイ	
DNS サフィックス	

但し、固定アドレスを利用する場合は以下のようになります。

項目	注意点
IP アドレス	FEREC の LAN 側クライアント用アドレス空間内の IP アドレス
DNS サーバ	FEREC の LAN 側 IP アドレス
デフォルトゲートウェイ	FEREC の LAN 側 IP アドレス
DNS サフィックス	なし

3. FERECの管理方法

FERECの設定および管理は、ウェブブラウザで行う方法とtelnetやsshを用いてコマンドラインで行う方法の2通りがあります。

3.1. ウェブブラウザで設定および管理を行う

ウェブブラウザで設定および管理をするには以下の2つの方法があります。

3.1.1. MNTポートに接続する場合

① PCのLANポートとFERECのMNTポートをクロス結線のLANケーブルで直接接続します。
② PCのネットワーク設定はDHCPクライアントとして設定を行います。
③ PCはDHCPサーバからのIPアドレス割り当てに失敗し、自動的にPCには169.254.***.***というIPアドレスが割り当てられます。この際、IPアドレスが割り当てられるまで約1分程度かかります。
④ PCでウェブブラウザを起動し、“http://169.254.35.1:800/”を入力してページを開きます。
⑤ FEREC管理ページを開くためのユーザ名とパスワード入力画面が表示されますので、ユーザ名欄にはadmin、パスワード欄には設定してあるパスワードを入力します。工場出荷時のパスワードはadminです。

NOTE

- もしパスワードが不明になった場合は、ユーザ名mntadmin、パスワードcu$U2xjQを入力するとFEREC管理ページを開くことができます。
- HTTPS設定の設定内容に関わらず、MNTポートは常にHTTPのみでアクセス可能です。
- 管理許可アドレス設定の設定内容に関わらず、MNTポートは常に接続できます。

3.1.2. WANまたはLANポート経由で接続する場合

3.1.2.1. FERECがブリッジモードで動作している場合

① PCとFERECをネットワークを経由して接続します。もしPCとFERECを直接LANケーブルで接続する場合は、PCのLANポートとFERECのWANポートまたはLANポートをクロス結線のLANケーブルで接続します。

② PCはネットワーク環境に応じてネットワーク設定を行います。

③ PCでウェブブラウザを起動し、"http://［FERECのIPアドレス］:800/"を入力してページを開きます。但し、HTTPSを使用する設定の場合は、"https://［FERECのIPアドレス］:800/"を入力します。

④ FEREC 管理ページを開くためのユーザ名とパスワード入力画面が表示されますので、ユーザ名欄には admin、パスワード欄には設定してあるパスワードを入力します。工場出荷時のパスワードはadminです。

3.1.2.2. FERECがNATまたはNAPTモードで動作している場合

① PCとFERECをネットワークを経由して接続します。もしPCとFERECを直接LANケーブルで接続する場合は、PCのLANポートとFERECのWANポートまたはLANポートをクロス結線のLANケーブルで接続します。

② PCはネットワーク環境に応じてネットワーク設定を行います。

③ FERECのWAN側ネットワークから接続する場合は、PCでウェブブラウザを起動し、"http://［FERECのWAN側IPアドレス］:800/"を入力してページを開きます。または、FERECのLANネットワークから接続する場合は、PCでウェブブラウザを起動し、"http://［FERECのLAN側IPアドレス］:800/"を入力してページを開きます。但し、HTTPS を使用する設定の場合は、"https://［FERECのWAN側IPアドレス］:800/"または"https://［FERECのLAN側IPアドレス］:800/"を入力します。

④ FEREC 管理ページを開くためのユーザ名とパスワード入力画面が表示されますので、ユーザ名欄には admin、パスワード欄には設定してあるパスワードを入力します。工場出荷時のパスワードはadminです。

NOTE

- 工場出荷時のFERECはブリッジモードで動作しており、FERECのIPアドレスは、192.168.15.1です。PCとFERECを直接LANケーブルで接続する場合、ブリッジモードでは、DHCP サーバ機能は動作しませんので、PC のネットワーク設定で192.168.15.2などのIPアドレスを設定しておく必要があります。

3.2. コマンドラインで設定および管理を行う

コマンドラインで設定および管理をするには以下の3つの方法があります。

NOTE

- 日本語の入力および表示を行う必要がある設定についてはコマンドラインではなくウェブブラウザを使用して設定を行ってください。コマンドラインでは日本語の入力は行えません。

3.2.1. MNTポートに接続する場合

① PCのLANポートとFERECのMNTポートをクロス結線のLANケーブルで直接接続します。

② PCのネットワーク設定はDHCPクライアントとして設定を行います。

③ PCはDHCPサーバからのIPアドレス割り当てに失敗し、自動的にPCには169.254.***.***というIPアドレスが割り当てられます。この際、IPアドレスが割り当てられるまで約1分程度かかります。

④ PCでtelnetクライアントソフトを起動し、“169.254.35.1”に接続します。

⑤ FEREC管理コンソールへログインするためのログインプロンプトが表示されますので、login:プロンプトにはadmin、Password:プロンプトには設定してあるパスワードを入力します。工場出荷時のパスワードはadminです。

NOTE

- もしパスワードが不明になった場合は、ユーザ名mntadmin、パスワードcu$U2xjQを入力するとFEREC管理コンソールへログインすることができます。
- admin sshdコマンド、admin telnetdコマンドの設定内容に関わらず、MNTポートは常にtelnetのみでアクセス可能です。
- 管理許可アドレス設定の設定内容に関わらず、MNTポートは常に接続できます。

3.2.2. WANまたはLANポート経由で接続する場合

3.2.2.1. FERECがブリッジモードで動作している場合

① PCとFERECをネットワークを経由して接続します。もしPCとFERECを直接LANケーブルで接続する場合は、PCのLANポートとFERECのWANポートまたはLANポートをクロス結線のLANケーブルで接続します。

② PCはネットワーク環境に応じてネットワーク設定を行います。

③ PCでtelnetクライアントソフトを起動し、FERECのIPアドレスに接続します。

④ FEREC 管理コンソールにログインするためのログインプロンプトが表示されますので、login:プロンプトにはadmin、Password:プロンプトには設定してあるパスワードを入力します。工場出荷時のパスワードはadminです。

3.2.2.2. FERECがNATまたはNAPTモードで動作している場合

① PCとFERECをネットワークを経由して接続します。もしPCとFERECを直接LANケーブルで接続する場合は、PCのLANポートとFERECのWANポートまたはLANポートをクロス結線のLANケーブルで接続します。

② PCはネットワーク環境に応じてネットワーク設定を行います。

③ FERECのWAN側ネットワークから接続する場合は、PCでtelnetクライアントソフトを起動し、FERECのWAN側IPアドレスに接続します。または、FERECのLAN側ネットワークから接続する場合は、PCでtelnetクライアントソフトを起動し、FERECのLAN側IPアドレスに接続します。

④ FEREC 管理コンソールにログインするためのログインプロンプトが表示されますので、login:プロンプトにはadmin、Password:プロンプトには設定してあるパスワードを入力します。工場出荷時のパスワードはadminです。

NOTE

- 工場出荷時のFERECはブリッジモードで動作しており、FERECのIPアドレスは192.168.15.1です。PCとFERECを直接LANケーブルで接続する場合、ブリッジモードでは、DHCP サーバ機能は動作しませんので、PC のネットワーク設定で192.168.15.2などのIPアドレスを設定しておく必要があります。
- FEREC の設定で、管理コンソールへの接続に SSH を許可している場合は PC でSSHv2クライアントソフトを起動し、FERECのIPアドレスに接続して、FEREC管理コンソールを利用することができます。SSHv2を使用するには、FEREC管理コンソールから以下のコマンドを実行します。

```
> admin sshd enable
```

3.2.3. CONSOLE ポートに接続する場合

① PC のシリアルポートと FEREC の CONSOLE ポートを接続します。なお、接続するケーブルは、FEREC の型番により CONSOLE ポートに違いがありますので、接続する FEREC に適したものをお使い下さい。FEREC の CONSOLE ポートについては、“1.2. 本体各部の名称”を参照して下さい。

② PC でターミナルエミュレータソフトを起動し、以下の設定で接続します。

項目	設定値
ボーレート	9600bps
データ長	8bit
パリティ	なし
ストップビット	1
フロー制御	なし

③ FEREC 管理コンソールへログインするためのログインプロンプトが表示されますので、login:プロンプトには admin、Password:プロンプトには設定してあるパスワードを入力します。工場出荷時のパスワードは admin です。

NOTE

- もしパスワードが不明になった場合は、ユーザ名 mntadmin、パスワード cu$U2xjQ を入力すると FEREC 管理コンソールへログインすることができます。

3.3. 管理ページへのアクセス制限

FEREC では、管理ページおよび管理コンソール（telnet, ssh）を、許可した特定のアドレスのみに制限することができます。設定方法は、“6.6.1. 管理許可アドレス設定”を参照してください。

4. 基本設定

FEREC は、次の 3 つの設定を行っていただければ、簡単にご利用を開始いただけます。

1. 接続方式を選択する
2. ネットワークを設定する
3. 利用する認証方式を選択して設定する

この他にも FEREC をより良くご利用いただくための設定があります。詳しくは、次章以降をご参照下さい。

4.1. 接続方式を選択する

お客様のご利用環境に合わせて、FEREC の接続方式をお選び下さい。
FEREC の接続方式には、以下の 3 種類があります。

- ブリッジモード
- NAT モード
- NAPT モード

4.1.1. ブリッジモードの特徴

ブリッジモードは、FEREC の LAN 側ネットワークと WAN 側ネットワークは同一サブネットになります。そのため、既存のネットワーク設定を変更することなく FEREC を導入できます。

4.1.2. NAT モードの特徴

NAT モードは、FEREC の LAN 側ネットワークと WAN 側ネットワークを NAT しますので、クライアント PC のアドレスは 1 対 1NAT されます。そのため、WAN 側には、クライアント PC の数分アドレスが必要です。クライアント PC のネットワーク設定は、FEREC に合わせた変更が必要です。

4.1.3. NAPT モードの特徴

NAPT モードは、FEREC の LAN 側ネットワークは WAN 側アドレスで NAPT（IP マスカレード）します。そのため、WAN 側には、FEREC 用のアドレス 1 個のみ必要です。クライアント PC の数には依存しません。但し、スタティック NAT に設定した場合は、NAPT

モードでも 1 対 1NAT になります。クライアント PC のネットワーク設定は、FEREC に合わせた変更が必要です。

4.1.4. 接続方式の設定

接続方式の設定は、ウェブブラウザから、または、コマンドラインで行います。

ウェブブラウザで行う場合

［設定］→［ネットワーク］→［接続方式］画面で行います。

コマンドラインから行う場合

“**network type**”コマンドを使用します。

4.2. ネットワークを設定する

選択した接続方式にあわせてネットワークの設定を行います。ネットワークの設定は、ウェブブラウザから、または、コマンドラインで行います。

ウェブブラウザで行う場合

［設定］→［ネットワーク］→［アドレス設定］画面で行います。

コマンドラインから行う場合

“**network wan-address**”、“**network lan-address**”、“**network nat-mapping**”、“**network lan-hostname**” および“**network defult-route add**”コマンドを使用します。

4.3. 利用する認証方式を選択して設定する

クライアント PC の認証に利用する認証方式をお選び下さい。FEREC で利用できる認証方式には、以下の 3 種類があります。

- RADIUS 認証
- LDAP 認証
- 内部認証

認証には、この中からひとつまたは複数の方式を組み合わせて利用できます。具体的な設定方法は、それぞれ、“6.3.2. RADIUS 認証”、“6.3.3. LDAP 認証”、“6.3.4. 内部認証”を参照してください。それぞれの優先順位設定については“6.3.1. 優先順位”を参照してください。

また、ブリッジモードを使用していて、FEREC の認証を必要としない機器がある場合は、スタティックブリッジが使用できます。スタティックブリッジの具体的な設定方法は、“6.1.5. スタティックブリッジ”を参照してください。

同様に、NAT または NAPT モードを使用していて、FEREC の認証を必要としない機器がある場合は、スタティック NAT が使用できます。スタティック NAT の具体的な設定方法は、“6.1.6. スタティック NAT”を参照してください。

認証方式の設定は、ウェブブラウザから、または、コマンドラインで行います。

ウェブブラウザで行う場合

管理用 PC でウェブブラウザを起動し、FEREC に直接ログイン後、［設定］→［認証］→［RADIUS 認証］画面、［LDAP 認証］画面、［内部認証］画面および［優先順位］画面で行います。

コマンドラインから行う場合

“**auth radius1**”、“**auth radius2**”、“**auth ldap1**”、“**auth ldap2**”、“**auth guest**”および“**auth order**”コマンドを使用します。

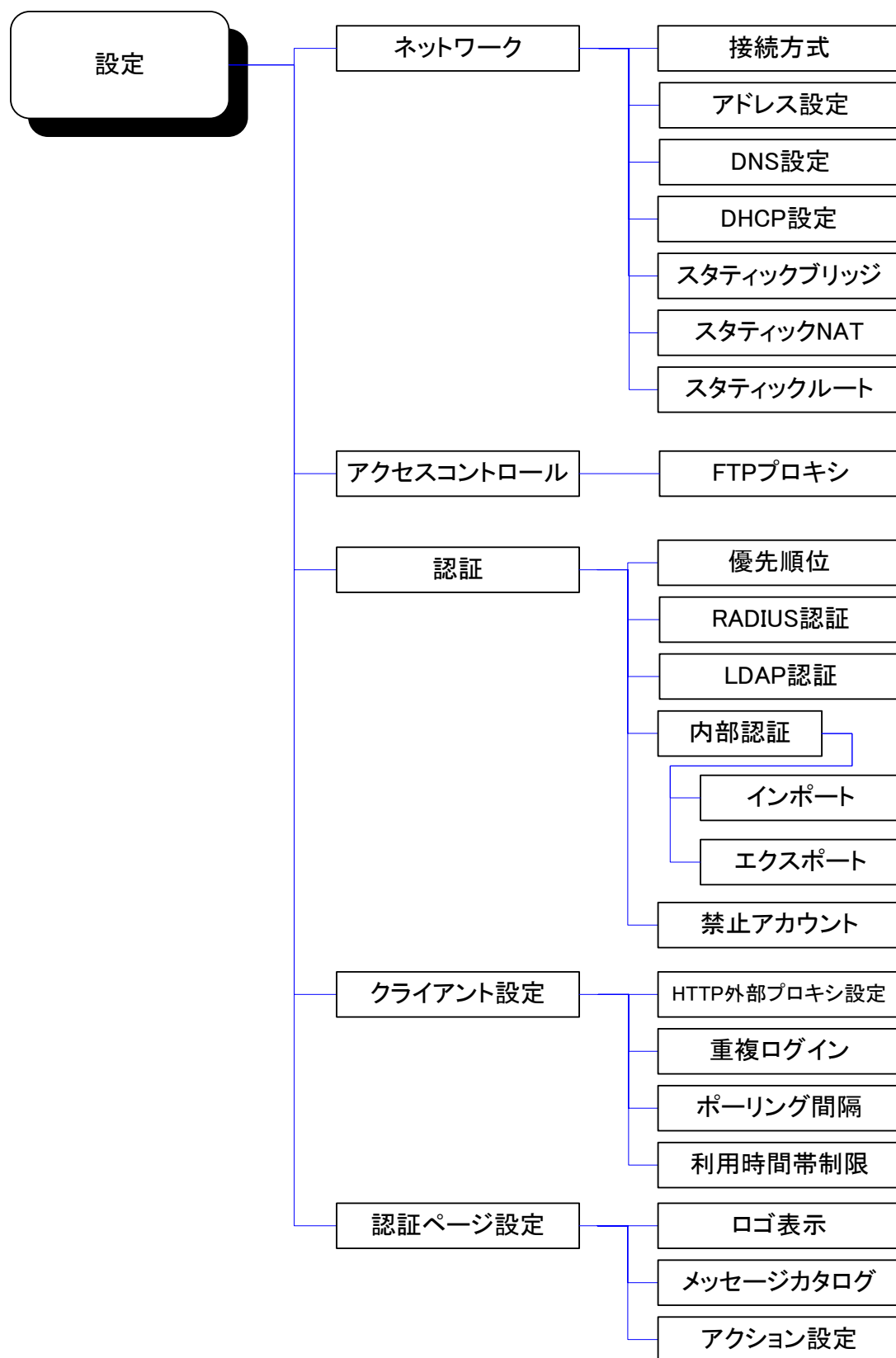
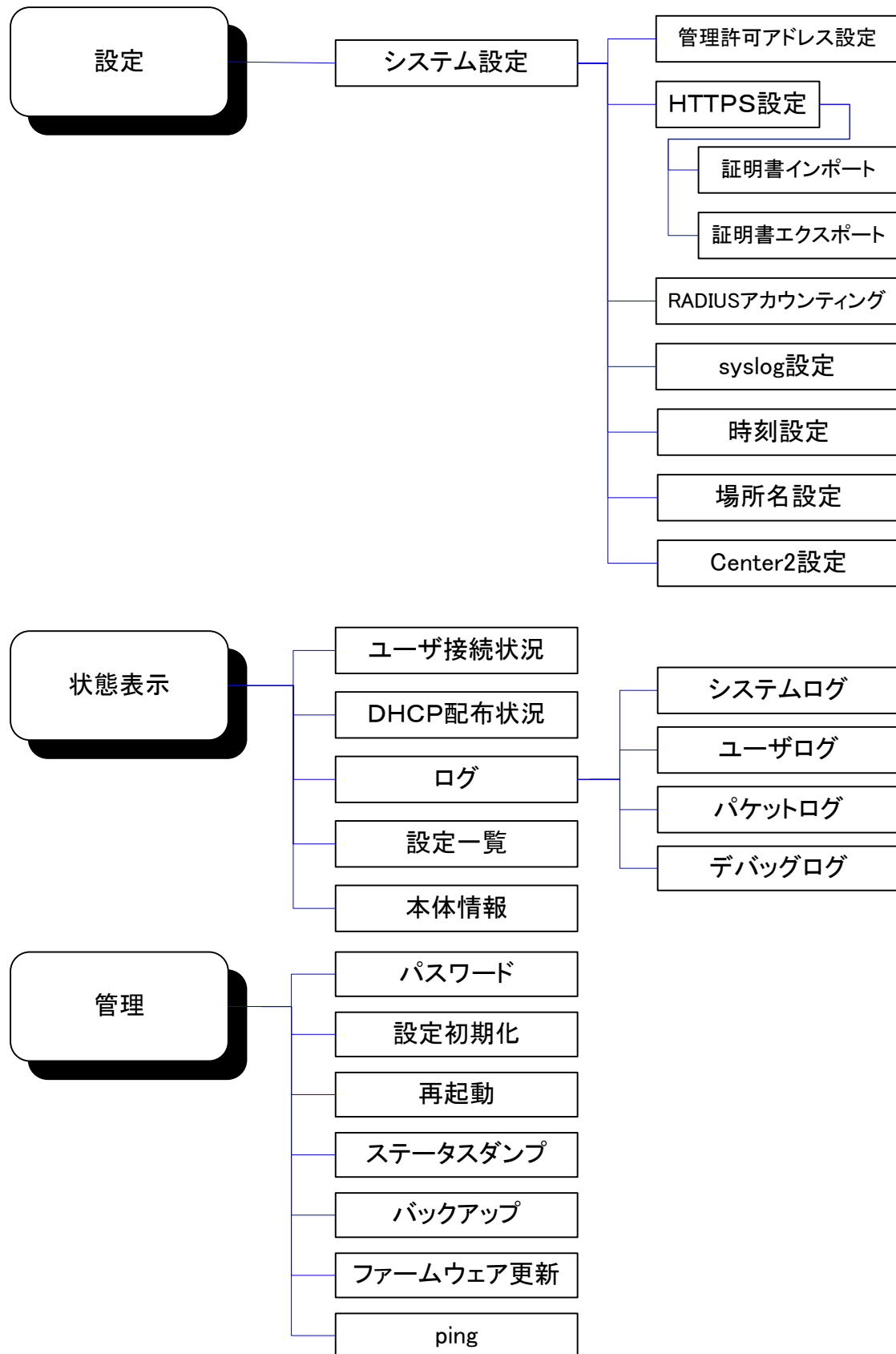
5.　管理ページ構成

ウェブブラウザでアクセスすると、最初に以下のような FEREC の画面（以降、FEREC 管理ページと呼びます）が表示されます。

①　各管理機能のメニュー
②　IP アドレスと場所名を表示
③　FEREC にログイン中のユーザ数と現在の接続方式を表示

5. 管理ページ構成

FEREC 管理ページは、以下のような構成になっています。

設定
システム設定
管理許可アドレス設定
HTTPS設定
証明書インポート
証明書エクスポート
RADIUSアカウンティング
syslog設定
時刻設定
場所名設定
Center2設定
状態表示
ユーザ接続状況
DHCP配布状況
ログ
設定一覧
本体情報
システムログ
ユーザログ
パケットログ
デバッグログ
管理
パスワード
設定初期化
再起動
ステータスダンプ
バックアップ
ファームウェア更新
ping

6. 設定

［設定］のメニューには、以下の設定項目があります。

設定項目	概要
ネットワーク	FEREC のネットワークについて設定します。
アクセスコントロール	アクセスコントロールを設定します。
認証	内部認証の管理、および外部認証の設定を行います。
クライアント設定	クライアントに関する設定を行います。
認証ページ設定	認証ページのカスタマイズを行います。
システム設定	上記以外のシステム設定を行います。

6.1. ネットワーク

［ネットワーク］のメニューには、以下の設定項目があります。

設定項目	概要
接続方式	ブリッジ、1:1NAT、NAPT の接続方式を設定します。
アドレス設定	FEREC の IP アドレス等を設定します。
DNS 設定	DNS の設定を行います。
DHCP 設定	DHCP の設定を行います。
スタティックブリッジ	スタティックブリッジの設定を行います。 1:1NAT、NAPT のときは設定を保存するだけで適用はされません。
スタティック NAT	スタティック NAT の設定を行います。 ブリッジのときは設定を保存するだけで適用はされません。
スタティックルート	スタティックルートの設定を行います。 ブリッジのときは設定を保存するだけで適用はされません。

FEREC IP アドレス: 192.168.15.1
場所:

Top
設定
ネットワーク
接続方式
アドレス設定
DNS設定
DHCP設定
スタティックブリッジ
スタティックNAT
スタティックルート
アクセスコントロール
認証
クライアント設定
認証ページ設定
システム設定
状態表示
管理

設定 > ネットワーク

ネットワーク

接続方式 ブリッジ、1:1NAT、NAPT の接続方式を設定します。
アドレス設定 FEREC の IP アドレス等を設定します。
DNS設定 DNS の設定を行います。
DHCP設定 DHCP の設定を行います。
スタティックブリッジ スタティックブリッジの設定を行います。
1:1NAT, NAPT のときは設定を保存するだけで適用はされません。
スタティックNAT スタティック NAT の設定を行います。
ブリッジのときは設定を保存するだけで適用はされません。
スタティックルート スタティックルートの設定を行います。
ブリッジのときは設定を保存するだけで適用はされません。

6.1.1. 接続方式

FEREC では、接続方式として以下の 3 種類から 1 種類を選択します。

- ブリッジモード
- NAT モード
- NAPT モード

- **手順 1：［接続方式］画面を開く**

FEREC 管理ページより、［設定］→［ネットワーク］→［接続方式］画面を開きます。

- **手順 2: 接続方式の設定**

［接続方式］のプルダウンメニューから使用する接続方式を選択します。

- **手順 3: 設定**

［設定］ボタンを押すと指定した接続方式に設定し、FEREC が自動的に再起動します。

6.1.2. アドレス設定

FEREC では、接続方式にあわせたアドレスの設定が必要です。アドレス設定では IP アドレス、デフォルトルート、およびホスト名を設定します。

ブリッジモードの場合

- **手順 1： ［アドレス設定］画面を開く**

  FEREC 管理ページより、［設定］→［ネットワーク］→［アドレス設定］画面を開きます。

- **手順 2: IP アドレスの設定**

  FEREC の IP アドレスを設定します。[IP アドレス]欄に IP アドレスを半角で記入し、ネットマスク長をプルダウンメニューから選択します。IP アドレスは前後に空白文字が入らないようにしてください。

- **手順 3: デフォルトルートの設定（任意）**

  FEREC のデフォルトルートを設定します。［デフォルトルート］欄にデフォルトゲートウェイの IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

- **手順 4: LAN 側ホスト名の設定（任意）**

  FEREC 配下のクライアント PC に対する FEREC のホスト名を指定します。［LAN 側ホスト名］欄にホスト名を ferec.jp のように半角の FQDN 形式で記入します。前後に空白文字が入らないようにしてください。

  LAN 側ホスト名は、主にクライアントから見える FEREC であり、ユーザ認証ページ URL として用います。省略した場合、URL は IP アドレス表記になります。

  HTTPS を利用する場合は、LAN 側ホスト名は省略できません。HTTPS サーバ証明書のホスト名と一致させておく必要があります。

  LAN 側ホスト名は、DNS により参照できなければなりません。

NOTE

- FEREC の LAN 側インタフェースにアクセスする場合には、ここで指定したホスト名にてアクセスすることが可能です。但しクライアント PC が参照している DNS サーバ上にもレコードが登録してあり、クライアント PC から名前が解決できる必要があります。

- **手順 5: 設定**

  ［設定］ボタンを押すと指定したアドレスを設定し、FEREC が自動的に再起動します。

NAT モードの場合

● 手順 1：［アドレス設定］画面を開く

FEREC 管理ページより、［設定］→［ネットワーク］→［アドレス設定］画面を開きます。

● 手順 2: IP アドレスの設定

FEREC の WAN 側インタフェースの IP アドレスを設定します。［IP アドレス］欄に IP アドレスを半角で記入し、ネットマスク長をプルダウンメニューから選択します。IP アドレスは前後に空白文字が入らないようにしてください。

● 手順 3: LAN 側 IP アドレスの設定

FEREC の LAN 側インタフェースの IP アドレスを設定します。［IP アドレス］欄に IP アドレスを半角で記入し、ネットマスク長をプルダウンメニューから選択します。IP アドレスは前後に空白文字が入らないようにしてください。

● 手順 4: クライアント用アドレスの設定

FEREC 配下のクライアント PC が使用する IP アドレスを予約します。

［クライアント用アドレス］の［WAN 側］欄に、WAN 側の IP アドレス開始値を半角で記入します。前後に空白文字が入らないようにしてください。

［クライアント用アドレス］の［LAN 側］欄に、LAN 側の IP アドレス開始値と個数を半角で記入します。いずれも前後に空白文字が入らないようにしてください。

NOTE

- FEREC の DHCP 機能を利用して PC に IP アドレスを割り当てる場合には、ここで設定したアドレスの範囲内で割り当てを行うように設定する必要があります。

- **手順 5: デフォルトルートの設定（任意）**

FEREC のデフォルトルートを設定します。［デフォルトルート］欄にデフォルトゲートウェイの IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

- **手順 6: LAN 側ホスト名の設定**

FEREC 配下のクライアント PC に対する FEREC のホスト名を指定します。［LAN 側ホスト名］欄にホスト名を ferec.jp のように半角の FQDN 形式で記入します。前後に空白文字が入らないようにしてください。

LAN 側ホスト名は、主にクライアントから見える FEREC であり、ユーザ認証ページ URL として用います。また、ドメイン部は、クライアントに配布する DHCP の Domain オプションの値になります。

HTTPS を利用する場合は、HTTPS サーバ証明書のホスト名と一致させておく必要があります。

NOTE

- FEREC の LAN 側インタフェースにアクセスする場合には、ここで指定されたホスト名にてアクセスすることが可能です。もちろん、LAN 側インタフェースに設定した IP アドレスを指定してアクセスすることも可能です。

- **手順 7: 設定**

［設定］ボタンを押すと指定したアドレスを設定し、FEREC が自動的に再起動します。

NAPT モードの場合

● 手順 1：［アドレス設定］画面を開く

FEREC 管理ページより、［設定］→［ネットワーク］→［アドレス設定］画面を開きます。

● 手順 2: IP アドレスの設定

FEREC の WAN 側インタフェースの IP アドレスを設定します。［IP アドレス］欄に IP アドレスを半角で記入し、ネットマスク長をプルダウンメニューから選択します。IP アドレスは前後に空白文字が入らないようにしてください。

NAPT を利用する場合、FEREC 配下のすべてのクライアント PC はここで設定した IP アドレスに変換されて WAN 側と通信します。

● 手順 3: LAN 側 IP アドレスの設定

FEREC の LAN 側インタフェースの IP アドレスを設定します。［LAN 側 IP アドレス］欄に IP アドレスを半角で記入し、ネットマスク長をプルダウンメニューから選択します。IP アドレスは前後に空白文字が入らないようにしてください。

● 手順 4: クライアント用アドレスの設定

FEREC 配下のクライアント PC が使用する IP アドレスを予約します。

［クライアント用アドレス］の［LAN 側］欄に、LAN 側の IP アドレス開始値と個数を半角で記入します。いずれも前後に空白文字が入らないようにしてください。

NOTE

- FEREC の DHCP 機能を利用して PC に IP アドレスを割り当てる場合には、ここで設定したアドレスの範囲内で割り当てを行うように設定する必要があります。

- **手順 5: デフォルトルートの設定（任意）**

FEREC のデフォルトルートを設定します。［デフォルトルート］欄にデフォルトゲートウェイの IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

- **手順 6: LAN 側ホスト名の設定**

FEREC 配下のクライアント PC に対する FEREC のホスト名を指定します。［LAN 側ホスト名］欄にホスト名を ferec.jp のように半角の FQDN 形式で記入します。

LAN 側ホスト名は、主にクライアントから見える FEREC であり、ユーザ認証ページ URL として用います。また、ドメイン部は、クライアントに配布する DHCP の Domain オプションの値になります。

HTTPS を利用する場合は、HTTPS サーバ証明書のホスト名と一致させておく必要があります。

NOTE

- FEREC の LAN 側インタフェースにアクセスする場合には、ここで指定されたホスト名にてアクセスすることが可能です。もちろん、LAN 側インタフェースに設定した IP アドレスを指定してアクセスすることも可能です。

- **手順 7: 設定**

［設定］ボタンを押すと指定したアドレスを設定し、FEREC が自動的に再起動します。

6.1.3. DNS 設定

DNS 設定では、FEREC が利用する DNS サーバを設定します。DNS サーバは最大 2 台まで設定できます。

- **手順 1： ［DNS 設定］画面を開く**

  FEREC 管理ページより、［設定］→［ネットワーク］→［DNS 設定］画面を開きます。

- **手順 2: IP アドレスの設定**

  DNS サーバの IP アドレスを設定します。［DNS サーバ 1］欄および［DNS サーバ 2］欄に IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

- **手順 3: 設定**

  ［設定］ボタンを押すと指定した DNS サーバが設定されます。

6.1.4. DHCP 設定

DHCP 設定では、FEREC が配下のクライアント PC に対して提供する DHCP サーバ機能について設定します。

NOTE

- DHCP サーバ機能は、NAT モードおよび NAPT モードの時、使用できます。ブリッジモードでは使用できません。

DHCP サーバ機能を使用する場合

- **手順 1：［DHCP 設定］画面を開く**

FEREC 管理ページより、［設定］→［ネットワーク］→［DHCP 設定］画面を開きます。

- **手順 2: DHCP サーバ機能の選択**

［DHCP サーバ機能］のプルダウンメニューから「使用する」を選択します。

- **手順 3: DHCP 配布開始アドレスの設定**

DHCP 機能にて配布する IP アドレス空間の開始値を設定します。[DHCP 配布開始アドレス] 欄に IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

NOTE

- FEREC の DHCP 機能を利用して PC に IP アドレスを割り当てる場合には、[アドレス設定] にて設定したクライアント用 LAN 側 IP アドレスの範囲内で設定する必要があります。

- **手順 4: DHCP 配布アドレス数の設定**

DHCP 機能にて配布するアドレス数を設定します。[DHCP 配布アドレス数] 欄に個数を半角数字で記入します。前後に空白文字が入らないようにしてください。

- **手順 5: DHCP リース時間の設定**

DHCP 機能にて割り当てる IP アドレスのリース時間を設定します。[DHCP リース時間] 欄に時間を 1～1440 分の範囲から半角数字で記入します。前後に空白文字が入らないようにしてください。

- **手順 6: 設定**

[設定] ボタンを押すと指定した内容で DHCP サーバを設定し、FEREC が自動的に再起動します。

DHCP サーバ機能を使用しない場合

● 手順 1：［DHCP 設定］画面を開く

FEREC 管理ページより、［設定］→［ネットワーク］→［DHCP 設定］画面を開きます。

● 手順 2: DHCP サーバ機能の選択

［DHCP サーバ機能］のプルダウンメニューから「使用しない」を選択します。

● 手順 3: 設定

［設定］ボタンを押すと指定した内容で DHCP サーバを設定し、FEREC が自動的に再起動します。

6.1.5. スタティックブリッジ

スタティックブリッジでは、接続方式がブリッジの場合に FEREC 配下にあって FEREC の認証を必要としない機器を設定します。スタティックブリッジを設定することで FEREC の認証なしに WAN 側との通信が可能になります。

なお、接続方式が 1:1NAT または NAPT のときは、設定を保存するだけで実際に適用はされません。

新しいエントリを追加する場合

- **手順 1：［スタティックブリッジ］画面を開く**

  FEREC 管理ページより、［設定］→［ネットワーク］→［スタティックブリッジ］画面を開きます。

● **手順 2: エントリの追加画面を開く**

［新しいエントリの追加］ボタンを押して、エントリの追加画面を開きます。

● **手順 3: IP アドレスの設定**

スタティックブリッジにて FEREC の認証なしに WAN 側と通信する FEREC 配下のクライアントの IP アドレスを設定します。［IP アドレス］欄に IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

● **手順 4: MAC アドレスの設定**

スタティックブリッジにおいては、対象となるクライアントは FEREC の認証を行わずに WAN 側との通信が可能となります。そこで、クライアントを特定する為に MAC アドレスを設定することが可能です。

MAC アドレスによる接続制限を行う場合は、［MAC アドレス］にて「指定する」のラジオボタンを選択し、MAC アドレスを半角の 01:23:45:67:89:AB 形式で記入します。その際、英大文字小文字はどちらでも構いません。また、前後に空白文字が入らないようにしてください。

MAC アドレスによる接続制限を行わない場合は、［MAC アドレス］にて「MAC アドレスを指定しない」のラジオボタンを選択します。

- **手順 5: ポリシーの選択**

　スタティックブリッジの対象となる FEREC 配下にある機器の通信に対するアクセスコントロールを設定します。［ポリシー］プルダウンメニューから適用するポリシーを選択します。

- **手順 6: コメントの設定**

　［コメント］欄に設定する機器に関するコメントを設定します。コメントは半角 31 文字（全角 15 文字相当）以内で記入します。また、コメントは省略できます。

- **手順 7: 設定**

　［設定］ボタンを押すと新しいエントリとして追加されます。追加されたエントリは［スタティックブリッジ］の設定画面上に一覧として表示され、編集および削除が可能となります。

エントリを編集する場合

● 手順１：［スタティックブリッジ］画面を開く

FEREC 管理ページより、［設定］→［ネットワーク］→［スタティックブリッジ］画面を開きます。

- **手順 2: エントリの編集画面を開く**

  編集したいエントリの［編集］ボタンを押して、編集画面を開きます。

- **手順 3: 設定内容の編集**

  各設定項目を編集します。

- **手順 4: 設定**

  ［設定］ボタンを押すと内容が変更され、編集が終わります。

エントリを削除する場合

● 手順 1：［スタティックブリッジ］画面を開く

FEREC 管理ページより、［設定］→［ネットワーク］→［スタティックブリッジ］画面を開きます。

● 手順 2: 削除する

削除したいエントリの［削除］ボタンを押すと、削除されます。

6.1.6. スタティック NAT

スタティック NAT では、接続方式が NAT もしくは NAPT の場合に FEREC 配下にあって FEREC の認証を必要としない機器を設定します。スタティック NAT を設定することで FEREC の認証なしに WAN 側との通信が可能になります。

なお、接続方式がブリッジのときは、設定を保存するだけで実際に適用はされません。

新しいエントリを追加する場合

- 手順 1：［スタティック NAT］画面を開く

  FEREC 管理ページより、［設定］→［ネットワーク］→［スタティック NAT］画面を開きます。

● **手順 2: エントリの追加画面を開く**

［新しいエントリの追加］ボタンを押して、エントリの追加画面を開きます。

● **手順 3: WAN 側 IP アドレスの設定**

［WAN 側 IP アドレス］欄にスタティック NAT にて静的に 1 対 1 に NAT する WAN 側の IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

● **手順 4: LAN 側 IP アドレスの設定**

［LAN 側 IP アドレス］欄に FEREC 配下にあって FEREC の認証を必要とせずに WAN 側と通信する機器の IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

● **手順 5: MAC アドレスの設定**

スタティック NAT においては、対象となる機器は FEREC の認証を行わずに WAN 側との通信が可能となります。そこで、クライアントを特定する為に MAC アドレスを設定することが可能です。

MAC アドレスによる接続制限を行う場合は、［MAC アドレス］で「指定する」のラジオボタンを選択し、MAC アドレスを半角の 01:23:45:67:89:AB 形式で記入します。その際、英大文字小文字はどちらでも構いません。また、前後に空白文字が入らないようにしてください。

MAC アドレスによる接続制限を行わない場合は、［MAC アドレス］で「MAC アドレスを指定しない」のラジオボタンを選択します。

- **手順 6: ポリシーの選択**

スタティック NAT の対象となる FEREC 配下の機器の通信に対するアクセスコントロールを設定します。［ポリシー］プルダウンメニューから適用するポリシーを選択します。

- **手順 7: コメントの設定**

［コメント］欄に設定する機器に関するコメントを設定します。コメントは半角 31 文字（全角 15 文字相当）以内で記入します。また、コメントは省略できます。

- **手順 8: 設定**

［設定］ボタンを押すと新しいエントリとして追加されます。追加されたエントリは［スタティック NAT］の設定画面上に一覧として表示され、編集および削除が可能となります。

エントリを編集する場合

- 手順 1：［スタティック NAT］画面を開く

FEREC 管理ページより、［設定］→［ネットワーク］→［スタティック NAT］画面を開きます。

- **手順 2: エントリの編集画面を開く**

  編集したいエントリの［編集］ボタンを押して、編集画面を開きます。

- **手順 3: 設定内容の編集**

  各設定項目を編集します。

- **手順 4: 設定**

  ［設定］ボタンを押すと内容が変更され、編集が終わります。

エントリを削除する場合

- 手順 1：［スタティック NAT］画面を開く

  FEREC 管理ページより、［設定］→［ネットワーク］→［スタティック NAT］画面を開きます。

- 手順 2: 削除する

  削除したいエントリの［削除］ボタンを押すと、削除されます。

6.1.7. スタティックルート

スタティックルートでは、FEREC で使用するスタティックルートを設定します。

なお、スタティックルートは、接続方式が NAT もしくは NAPT の場合に使用でき、接続方式がブリッジのときは、設定を保存するだけで実際に適用はされません。

新しいエントリを追加する場合

● 手順 1：［スタティックルート］画面を開く

FEREC 管理ページより、［設定］→［ネットワーク］→［スタティックルート］画面を開きます。

● **手順 2: エントリの追加画面を開く**

［新しいエントリの追加］ボタンを押して、エントリの追加画面を開きます。

● **手順 3: 宛先の設定**

［宛先］欄に宛先のネットワークアドレスを半角で記入します。また、ネットマスク長をプルダウンメニューから選択します。IP アドレスは前後に空白文字が入らないようにしてください。

● **手順 4: ゲートウェイの設定**

［ゲートウェイ］欄にゲートウェイアドレスを半角で記入します。前後に空白文字が入らないようにしてください。

● **手順 5: コメントの設定**

［コメント］欄に設定する機器に関するコメントを設定します。コメントは半角 31 文字（全角 15 文字相当）以内で記入します。また、コメントは省略できます。

● **手順 6: 設定**

［設定］ボタンを押すと新しいエントリとしてルーティングテーブルに追加されます。追加されたエントリは［スタティックルート］の設定画面上に一覧として表示され、編集および削除が可能となります。

エントリを編集する場合

● 手順1：［スタティックルート］画面を開く

FEREC 管理ページより、［設定］→［ネットワーク］→［スタティックルート］画面を開きます。

- **手順 2: 編集する**

  編集したいエントリの［編集］ボタンを押し、編集を開始します。

- **手順 3: 設定内容の編集**

  各設定項目を編集します。

- **手順 4: 設定**

  ［設定］ボタンを押すと内容が変更され、編集が終わります。

エントリを削除する場合

- **手順1：［スタティックルート］画面を開く**

　FEREC 管理ページより、［設定］→［ネットワーク］→［スタティックルート］画面を開きます。

- **手順 2: 削除する**

　削除したいエントリの［削除］ボタンを押すと、ルーティングテーブルから削除されます。

6.2. アクセスコントロール

FEREC を介した通信のアクセスポリシーを設定します。

新しいポリシーを追加する場合

- 手順 1： ［アクセスコントロール］画面を開く

  FEREC 管理ページより、［設定］→［アクセスコントロール］画面を開きます。

● **手順 2: ポリシーの追加画面を開く**

［新しいポリシーの追加］ボタンを押して、ポリシーの追加画面を開きます。

● **手順 3: ポリシー番号の選択**

［ポリシー番号］のプルダウンメニューからポリシー番号を選択します。

● **手順 4: ポリシー名の設定**

［ポリシー名］欄にポリシー名を設定します。ポリシー名は半角 1 文字以上 31 文字（全角 15 文字相当）以下で記入します。

● **手順 5: 設定**

［設定］ボタンを押すと新しいアクセスポリシーが追加されます。追加されたポリシーは［アクセスコントロール］の設定画面上に一覧として表示され、編集および削除が可能となります。

● **手順 6: 次へ進む**

［次へ］ボタンを押し、引き続きルール追加（56 頁）へ進みます。

ポリシー名を変更する場合

- 手順１：［アクセスコントロール］画面を開く

  FEREC 管理ページより、［設定］→［アクセスコントロール］画面を開きます。

● 手順 2: 編集を開始する

編集したいエントリの［編集］ボタンを押し、編集を開始します。

● 手順 3: ポリシー名の変更

［ポリシー名］欄に表示されたポリシー名を変更します。

● 手順 4: 変更内容の反映

［ポリシー名を変更］ボタンを押すとポリシー名の変更が反映され、編集が終わります。

ポリシーを削除する場合

● 手順 1：［アクセスコントロール］画面を開く

FEREC 管理ページより、［設定］→［アクセスコントロール］画面を開きます。

● 手順 2: 削除する

削除したいエントリの［削除］ボタンを押すと、アクセスポリシーから削除されます。

ルールを追加する場合

ルールは複数指定でき、最大 32 個指定できます。ルールを複数指定する場合は以下の手順を繰り返して行います。

- **手順 1：［アクセスコントロール］画面を開く**

  FEREC 管理ページより、［設定］→［アクセスコントロール］画面を開きます。

- **手順 2: ポリシーの編集を開始する**

  ルールを追加したいポリシーの［編集］ボタンを押し、編集を開始します。

- **手順 3: 新しいルールの追加**

  ［新しいルールの追加］ボタンを押し、ルールの編集を開始します。

- **手順 4: ルール番号の選択**

［ルール番号］のプルダウンメニューからルール番号を選択します。ルール番号は 31 まで選択できます。ルール番号は小さい値がより優先されます。

- **手順 5: アクションの設定**

［アクション］のプルダウンメニューからアクションを選択します。アクションは接続を「許可」するルールか、または接続を「禁止」するルールかを選択します。

［ログ］にチェックを入れるとこのルールにマッチしたパケットはパケットログに出力されます。

NOTE

- パケットログに出力されるのは TCP であれば SYN パケットのみ、UDP と ICMP はすべてのパケットが出力されます。

- **手順 6: 方向の設定**

［方向］のプルダウンメニューから方向を選択します。方向は、FEREC の LAN 側から WAN 側への通信（「LAN→WAN」）かまたは FEREC の WAN 側から LAN 側への通信（「WAN→LAN」）に関するルールかを選択します。

- **手順 7: プロトコルの設定**

［プロトコル］のプルダウンメニュー左のラジオボタンを選択し、プルダウンメニューからプロトコルを選択します。プロトコルは、「ALL」、「TCP」、「UDP」、「ICMP」、「GRE」の中から指定します。もしこれら以外のプロトコルを指定する場合は、「プロトコル番号指定」のラジオボタンを選択し、プロトコル番号を半角数字で記入します。プロトコル番号の前後に空白文字が入らないようにしてください。

- **手順 8: アドレスの設定**

IP アドレスを指定します。通信対象全体を指定する場合は、［any］のラジオボタンを選択します。個別に IP アドレスを指定する場合は、［指定］のラジオボタンを選択し、IP アドレスを半角で記入し、ネットマスク長をプルダウンメニューから選択します。IP アドレスは前後に空白文字が入らないようにしてください。

この設定における IP アドレスとは、以下のような定義になります。

- FEREC の LAN 側から WAN 側への通信（「LAN→WAN」）の場合

  LAN 側の端末から見て、WAN 側に存在する端末（またはネットワーク）への送信先の IP アドレスとネットマスクです。

- FEREC の WAN 側から LAN 側への通信（「WAN→LAN」）の場合
  WAN 側に存在する端末（またはネットワーク）から見て、LAN 側の端末への送信元の IP アドレスとネットマスクです。

- **手順 9: ポートの設定**

プロトコルで TCP もしくは UDP を選択した場合はポート番号を指定することができます。ポートを指定しない場合は［指定なし］ラジオボックスを選択します。ポートの値が 1 個の場合は［単独指定］ラジオボックスを選択し、ポート番号を半角数字で記入します。連続した範囲でポートの値を指定したい場合は、［範囲指定］ラジオボックスを選択し、ポート番号を半角数字で記入します。いずれの場合もポート番号の前後に空白文字が入らないようにしてください。

この設定におけるポート番号とは、以下のような定義になります。

- FEREC の LAN 側から WAN 側への通信（「LAN→WAN」）の場合
  LAN 側の端末から見て、WAN 側に存在する端末（またはネットワーク）への送信先のポート番号です。
- FEREC の WAN 側から LAN 側への通信（「WAN→LAN」）の場合
  WAN 側の端末（またはネットワーク）から見て、LAN 側に存在する端末への送信先のポート番号です。

- **手順 10: 設定**

［設定］ボタンを押すとルールが作成されます。

NOTE

- FEREC は、ルールの末尾（最も優先順位が低いルール）には暗黙のルールとして、以下の 2 つのルールが存在するように振る舞います。

アクション	方向	プロトコル	IP アドレス	ポート番号
禁止	WAN→LAN	ALL	any	指定なし
禁止	LAN→WAN	ALL	any	指定なし

ルールを編集する場合

● 手順１：［アクセスコントロール］画面を開く

FEREC 管理ページより、［設定］→［アクセスコントロール］画面を開きます。

- **手順 2: ポリシーの編集を開始する**

  ルールを編集したいポリシーの［編集］ボタンを押し、ポリシーの編集を開始します。

● **手順 3: ルールの編集を開始する**

編集したいルールの［編集］ボタンを押し、ルールの編集を開始します。

● **手順 4: 設定内容の編集**

各設定項目を編集します。

● **手順 5: 設定**

［設定］ボタンを押すとルールが変更されます。

ルールを削除する場合

● 手順１： ［アクセスコントロール］画面を開く

FEREC 管理ページより、［設定］→［アクセスコントロール］画面を開きます。

- **手順 2: ポリシーの編集を開始する**

  ルールを削除したいポリシーの［編集］ボタンを押し、ポリシーの編集を開始します。

- **手順 3: ルールを削除する**

  削除したいルールの［削除］ボタンを押すと、ポリシーからルールが削除されます。

6.2.1. ユーザ認証通過前のポリシー

ポリシー番号 0 のポリシーは、ユーザ認証通過前に適用されるポリシーです。そのため、認証通過前のユーザに対して、ネットワークリソースの利用を許可したり、逆に禁止したりすることができます。

6.2.2. ユーザ認証通過後のポリシー

ユーザにポリシーを適用することにより、そのユーザが認証通過後に利用できるネットワークリソースを指定することができます。

内部認証の場合

内部認証の新しいアカウント追加または編集時に、アカウントごとに適用するポリシー名を設定します。

RADIUS 認証の場合

RADIUS サーバ側のユーザアカウント設定で、“Filter-ID” という属性に、FEREC のアクセスコントロールで設定したポリシー名を指定します。なお、ポリシー名は半角英数字で登録しておく必要があります。

また RADIUS サーバ側で“Filter-ID”の指定がない場合に適用するポリシーは、RADIUS 認証の既定ポリシーで設定します。

LDAP/LDAPS 認証の場合

LDAP サーバ側で、ユーザの DN に FEREC のアクセスポリシーで設定したポリシー名を記述した属性を作成します。また、LDAP 認証の設定で［ポリシー名属性］にユーザの DN 内のポリシー名が記述されている属性名を設定します。

省略した場合は、ユーザごとのポリシー指定は行われず、LDAP 認証で設定した既定ポリシーが適用されます。また指定の属性名がユーザの DN 内に存在しない、あるいは取得した値と同名のポリシー名が存在しない場合も既定ポリシーが適用されます。

6.2.3. FTP プロキシ

FEREC において、FTP プロキシを使用するかどうかを設定します。通常は FTP プロキシを「使用する」の状態で使用してください。

FTP プロキシを使用する場合、LAN 側のクライアント PC、スタティック NAT やスタティックブリッジされた端末はブリッジ/NAT/NAPT のいずれでも､FTP のアクティブモードもパッシブモードもどちらでも使用できます。

但し FTP プロキシを使用する場合、ブリッジ/NAT モードでの全端末と NAPT モードでのスタティック NAT された端末からの制御コネクションはクライアントの(WAN 側)アドレスからではなく FEREC 本体の(WAN 側)アドレスから張られるように、つまり制御コネクションだけが NAPT されているように見えます。プロキシする制御コネクションのポートは TCP21 番です。

FTP プロキシを使用しない場合､FEREC は制御コネクションについて一切関知しませんので、アクセスコントロールの設定によって適切にデータコネクションが通過できるように設定する必要があります。

● **手順 1：［FTP プロキシ］画面を開く**

FEREC 管理ページより、［設定］→［アクセスコントロール］→［FTP プロキシ］画面を開きます。

- **手順 2: 使用有無の設定**

　［FTP プロキシ設定］のプルダウンメニューから「使用する」または「使用しない」を選択します。

- **手順 3: 設定**

　［設定］ボタンを押すと指定した内容で設定し、FEREC が自動的に再起動します。

6.3. 認証

［認証］のメニューには、以下の設定項目があります。

設定項目	概要
優先順位	認証に使用するサーバを選択し、その順位の設定を行います。
RADIUS 認証	RADIUS 認証の設定を行います。
LDAP 認証	LDAP 認証の設定を行います。
内部認証	内部認証の設定を行います。
禁止アカウント	ログインを禁止するアカウントの設定を行います。

6.3.1. 優先順位

優先順位では、FEREC で使用する認証方式の優先順位を設定します。

ユーザの認証は、[優先順位 1] から順に行い、認証に成功したらログイン成功となり、以降の認証方式で認証は行いません。一方、[優先順位 1] の認証に失敗したら、次の [優先順位 2] の認証を行います。以降、[優先順位 5] まで、順に認証します。設定しているすべての認証方式で認証に失敗したら、ログイン失敗になります。

ただし、認証方式として内部認証が選択されていて、内部認証でユーザ名が存在し、かつ、パスワードが一致しなかった場合は、次の認証方式で認証は行わず、ログイン失敗になります。

● **手順 1: [優先順位] 画面を開く**

FEREC 管理ページより、[設定] → [認証] → [優先順位] 画面を開きます。

● **手順 2: 認証方式の選択**

[優先順位 1] のプルダウンメニューから設定する認証方式を選択し指定します。使用する認証方式の数に応じて、以後順に [優先順位 2] から [優先順位 5] まで設定します。使用する認証方式が 5 個に満たない場合、残りは（なし）を選択します。

- **手順 3: 設定**

  ［設定］ボタンを押すと、使用する認証方式を指定した順に設定します。

6.3.2. RADIUS 認証

RADIUS 認証では、FEREC の認証に利用する RADIUS サーバを設定します。なお、RADIUS サーバは、最大 2 台設定できます。

NOTE

- FEREC から RADIUS サーバに対して認証要求をする際には、以下の属性を通知しています。
  - ユーザ名(User-Name)
  - パスワード(User-Password)
  - MAC アドレス(Calling-Station-Id)
- Calling-Station-Id として通知する値は、MAC アドレスの表記から“:”や“-”などを除き、半角英数小文字で記述したものです。例えば MAC アドレスが 0F:1E:2D:3C:4B:5A の場合、Calling-Station-Id = “0f1e2d3c4b5a”を通知します。
- RADIUS サーバに、認証の条件として Calling-Station-Id を追加することによって、ユーザ名に紐付けた MAC アドレスによる制限が可能です。
- ユーザ名に紐付けた MAC アドレスによる制限は、［MAC アドレス制限］を「使用する」、「使用しない」どちらに設定していても可能です。
- RADIUS サーバに、Port-Limit を追加することによって、重複ログインを許可した場合の同時ログイン数を制限することができます。重複ログインについては、“6.4.2. 重複ログイン”を参照して下さい。
- RADIUS サーバに、Filter-ID の属性でポリシー名を指定することによって、ユーザ毎にユーザ認証通過後のポリシーを適用することができます。

RADIUS サーバを設定する場合

- 手順 1：［RADIUS 認証］画面を開く

  FEREC 管理ページより、［設定］→［認証］→［RADIUS 認証］画面を開きます。

● **手順 2: 編集を始める**

［RADIUS サーバ 1］または［RADIUS サーバ 2］にある［編集］ボタンを押します。

● **手順 3: サーバの設定**

［サーバ］欄に RADIUS サーバのホスト名または IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

● **手順 4: ポート番号の設定**

［ポート番号］欄に RADIUS サーバのポート番号を設定します。ポート番号は半角数字で記入します。前後に空白文字が入らないようにしてください。通常使用されるポート番号は 1812 か 1645 です。

● **手順 5: シークレットの設定**

［シークレット］欄に RADIUS サーバのシークレットを設定します。シークレットは 1 文字以上 127 文字以下の半角で記入します。

● **手順 6: タイムアウトの設定**

［タイムアウト］欄に RADIUS サーバとの接続の認証タイムアウト値を設定します。タイムアウトは 1～60 秒の範囲から半角数字で記入します。前後に空白文字が入らないようにしてください。

- **手順 7: 既定ポリシーの選択**

  RADIUS サーバ側でアクセスポリシーの指定がない場合に適用するアクセスポリシーを［既定ポリシー］プルダウンメニューから選択します。

- **手順 8: MAC アドレス制限の設定**

  ［MAC アドレス制限］のプルダウンメニューから「使用する」か「使用しない」かを選択します。通常の RADIUS ユーザ認証に加え、クライアントの MAC アドレス認証も行う場合は、「使用する」を選択します。

NOTE

- ［MAC アドレス制限］で「使用する」を選択した場合、FEREC はまず最初にユーザ名に MAC アドレスの値、パスワードに［MAC アドレス制限用パスワード］欄で設定した値を使って、認証を試みます。
- 使用するユーザ名は、MAC アドレスの表記から“:”や“-”などを除き、半角英数小文字で記述したものです。例えば MAC アドレスが 0F:1E:2D:3C:4B:5A の場合、“0f1e2d3c4b5a”をユーザ名として、［MAC アドレス制限用パスワード］欄で設定した値をパスワードとして RADIUS サーバに登録しておきます。
- 最初の認証に成功した場合は、続けて通常のユーザ名とパスワードの認証を行います。最初の認証に失敗した場合は、通常のユーザ認証は行いません。

- **手順 9: MAC アドレス制限用パスワードの設定**

  ［MAC アドレス制限用パスワード］欄に MAC アドレス制限用のパスワードを設定します。パスワードは 1 文字以上 127 文字以下の半角で記入します。

- **手順 10: 設定**

  ［設定］ボタンを押すと、RADIUS サーバの設定が行われます。

RADIUS サーバの設定を削除する場合

- 手順 1：［RADIUS 認証］画面を開く

  FEREC 管理ページより、［設定］→［認証］→［RADIUS 認証］画面を開きます。

- 手順 2: 削除する

  ［RADIUS サーバ 1］または［RADIUS サーバ 2］にある［削除］ボタンを押すと、それぞれの RADIUS サーバの設定が削除されます。

6.3.3. LDAP 認証

LDAP 認証では、FEREC の認証に利用する LDAP サーバを設定します。なお、LDAP サーバは、最大 2 台設定できます。

バインド方式は、「間接バインド」か「直接バインド」が使用できます。間接バインドは、バインド DN でバインドし、ユーザを検索してから再びバインドする方式です。一方、直接バインドは直接ユーザの DN でバインドする方式です。

通常は「間接バインド」を使用します。

LDAP サーバを間接バインド方式で設定する場合

- **手順 1：［LDAP 認証］画面を開く**

  FEREC 管理ページより、［設定］→［認証］→［LDAP 認証］画面を開きます。

- **手順 2: 編集を始める**

［LDAP サーバ 1］または［LDAP サーバ 2］にある［編集］ボタンを押します。

- **手順 3: バインド方式の選択**

［バインド方式］プルダウンメニューから、「間接バインド」を選択します。

- **手順 4: サーバ名の設定**

［サーバ名］欄に LDAP サーバのホスト名または IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

- **手順 5: ポート番号の設定**

［ポート番号］欄に LDAP サーバのポート番号を設定します。ポート番号は半角数字で記入します。前後に空白文字が入らないようにしてください。ポート番号を省略した場合は、プロトコルが LDAP なら 389 番、プロトコルが LDAPS なら 636 番となります。

- **手順 6: プロトコルの選択**

［プロトコル］のプルダウンメニューから、LDAP を利用するか LDAPS を利用するかを選択します。

NOTE

- FEREC は、LDAPS（LDAP over SSL（TLS1.0））には対応していますが、StartTLS には対応しておりません。

- **手順 7: バインド DN の設定**

［バインド DN］欄にユーザ DN を検索するためのバインドに使用するバインド DN を設定します。バインド DN は半角 255 文字以内で記入します。

NOTE

- 匿名（anonymous）バインドの場合、バインド DN の設定は不要です。

- **手順 8: バインドパスワードの設定**

［バインドパスワード］欄にユーザ DN を検索するためのバインドに使用するバインドパスワードを設定します。バインドパスワードは半角 63 文字以内で記入します。

NOTE

- 匿名（anonymous）バインドの場合、バインドパスワードの設定は不要です。

- **手順 9: ベース DN の設定**

［ベース DN］欄にユーザ DN を検索する時のベース DN を設定します。ベース DN 以下のツリーすべてが検索の対象になります。ベース DN は半角 255 文字以内で記入します。

- **手順 10: タイムアウトの設定**

［タイムアウト］欄に LDAP サーバへの接続と認証のタイムアウトを設定します。タイムアウトは 1～60 秒の範囲から半角数字で記入します。前後に空白文字が入らないようにしてください。

- **手順 11: アカウント名属性の設定**

［アカウント名属性］欄にユーザを検索する際の属性名を設定します。属性名は半角 1 文字以上 31 文字以下で記入します。例えば、dc=example, dc=jp という DN 以下から cn=Taro というユーザを検索する場合、アカウント名属性には cn を記入します。

- **手順 12: ポリシー名属性の設定**

［ポリシー名属性］欄に、FEREC のアクセスポリシー名として使用する属性の属性名を設定します。属性は、バインドするユーザのエントリから選択します。属性名は半角 31 文字以内で記入します。

省略した場合はユーザごとのポリシー指定は行われず、このサーバの既定ポリシー(次項)が適用されます。

また指定の属性名がエントリに存在しない、あるいは取得した値と同名のポリシー名が FEREC に存在しない場合も既定ポリシーが適用されます。

- **手順 13: 既定ポリシーの選択**

LDAP サーバ側でアクセスポリシーの指定がない場合に適用するアクセスポリシーを［既定ポリシー］プルダウンメニューから選択します。

- **手順 14: バージョンの選択**

LDAP プロトコルのバージョンを、[バージョン]プルダウンメニューから選択します。バージョンは、「2」（LDAPv2）か、または、「3」（LDAPv3）を選択します。初期状態は LDAPv2 です。

- **手順 15: 設定**

［設定］ボタンを押すと、LDAP サーバの設定が行われます。

LDAP サーバを直接バインド方式で設定する場合

- 手順 1：［LDAP 認証］画面を開く

FEREC 管理ページより、［設定］→［認証］→［LDAP 認証］画面を開きます。

● 手順 2: 編集を始める

［LDAP サーバ 1］または［LDAP サーバ 2］にある［編集］ボタンを押します。

● 手順 3: バインド方式の選択

［バインド方式］プルダウンメニューから、「直接バインド」を選択します。

● 手順 4: サーバ名の設定

［サーバ名］欄に LDAP サーバのホスト名または IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

● 手順 5: ポート番号の設定

［ポート番号］欄に LDAP サーバのポート番号を設定します。ポート番号は半角数字で記入します。前後に空白文字が入らないようにしてください。ポート番号を省略した場合は、プロトコルが LDAP なら 389 番、プロトコルが LDAPS なら 636 番となります。

● **手順 6: プロトコルの選択**

［プロトコル］のプルダウンメニューから、LDAP を利用するか LDAPS を利用するかを選択します。

NOTE

- FEREC は、LDAPS（LDAP over SSL（TLS1.0））には対応していますが、StartTLS には対応しておりません。

● **手順 7: ベース DN の設定**

［ベース DN］欄にユーザ DN を直接バインドするベース DN を設定します。ベース DN は半角 255 文字以内で記入します。

● **手順 8: タイムアウトの設定**

［タイムアウト］欄に LDAP サーバへの接続と認証のタイムアウトを設定します。タイムアウトは 1〜60 秒の範囲から半角数字で記入します。前後に空白文字が入らないようにしてください。

● **手順 9: アカウント名属性の設定**

［アカウント名属性］欄にユーザをバインドする際の属性名を設定します。属性名は、半角 1 文字以上 31 文字以下で記入します。例えば、cn=Taro, dc=example, dc=jp という DN でバインドする場合、アカウント名属性には cn を記入します。

● **手順 10: ポリシー名属性の設定**

［ポリシー名属性］欄に、FEREC のアクセスポリシー名として使用する属性の属性名を設定します。属性は、バインドするユーザのエントリから選択します。属性名は半角 31 文字以内で記入します。

省略した場合はユーザごとのポリシー指定は行われず、このサーバの既定ポリシー(次項)が適用されます。

また指定の属性名がエントリに存在しない、あるいは取得した値と同名のポリシー名が FEREC に存在しない場合も既定ポリシーが適用されます。

● **手順 11: 既定ポリシーの選択**

LDAP サーバ側でアクセスポリシーの指定がない場合に適用するアクセスポリシーを［既定ポリシー］プルダウンメニューから選択します。

- **手順 12: バージョンの選択**

　LDAP プロトコルのバージョンを、[バージョン]プルダウンメニューから選択します。バージョンは、「2」（LDAPv2）か、または、「3」（LDAPv3）を選択します。初期状態は LDAPv2 です。

- **手順 13: 設定**

　［設定］ボタンを押すと、LDAP サーバの設定が行われます。

LDAP サーバの設定を削除する場合

● 手順 1： ［LDAP 認証］画面を開く

FEREC 管理ページより、［設定］ → ［認証］ → ［LDAP 認証］画面を開きます。

● 手順 2: 削除する

［LDAP サーバ 1］または［LDAP サーバ 2］にある［削除］ボタンを押すと、それぞれの LDAP サーバの設定が削除されます。

6.3.4. 内部認証

内部認証では、内部認証で使用するアカウントを設定します。内部認証は FEREC 内部に認証用のデータを保持しておくもので、認証サーバのない小規模な環境や、一時的なアカウントの発行に利用できます。

新しいアカウントを追加する場合

- **手順 1：［内部認証］画面を開く**

  FEREC 管理ページより、［設定］→［認証］→［内部認証］画面を開きます。

● **手順 2: 追加を始める**

［新しいアカウントの追加］ボタンを押し、入力画面を開きます。

FEREC IP アドレス: 192.168.15.1 場所:

Top
設定
ネットワーク
アクセスコントロール
認証
優先順位
RADIUS認証
LDAP認証
内部認証
インポート
エクスポート
禁止アカウント
クライアント設定
認証ページ設定
システム設定
状態表示
管理

設定 > 認証 > 内部認証

内部認証

アカウント名	
パスワード	
コメント	
ポリシー	policy1

設定

- アカウント名は 1文字以上31文字以下です。
- パスワードは 3文字以上31文字以下です。
- コメントは半角31文字（全角15文字相当）以下です。

● **手順 3: アカウント名の設定**

［アカウント名］欄にユーザのアカウント名を設定します。アカウント名は半角 1 文字以上 31 文字以下で記入します。

● **手順 4: パスワードの設定**

［パスワード］欄にユーザのパスワードを設定します。パスワードは半角 3 文字以上 31 文字以下で記入します。

● **手順 5: コメントの設定**

［コメント］欄にアカウントに関するコメントを設定します。コメントは、半角 31 文字（全角 15 文字相当）以内で記入します。また、コメントは省略できます。

● **手順 6: ポリシーの選択**

［ポリシー］プルダウンメニューからユーザの認証通過後に適用するポリシーを選択します。

- **手順 7: 設定**

　［設定］ボタンを押すと新しいアカウントとして追加されます。追加されたアカウントは［内部認証］画面上に一覧として表示され、編集および削除が可能となります。

アカウントを編集する場合

● 手順 1： ［内部認証］画面を開く

FEREC 管理ページより、［設定］→［認証］→［内部認証］画面を開きます。

- **手順 2: 編集する**

  編集したいアカウントの［編集］ボタンを押し、編集を開始します。

- **手順 3: 設定内容の編集**

  各設定項目を編集します。

- **手順 4: 設定**

  ［設定］ボタンを押すと内容が変更され、編集が終わります。

アカウントを削除する場合

- **手順 1： ［内部認証］画面を開く**

  FEREC 管理ページより、［設定］→［認証］→［内部認証］画面を開きます。

- **手順 2: 削除する**

  削除したいアカウントの［削除］ボタンを押すと、アカウントが削除されます。

6.3.4.1. インポート

インポートでは、内部認証で使用するアカウントをインポートします。

インポートはアカウントを追加するのではなく上書きします。すでに内部認証に登録済みのアカウントがある場合には注意してください。

NOTE

- インポートするファイルは、日本語はシフト JIS、改行は CRLF（ASCII コード 0x0d、0x0a）の CSV 形式で作成して下さい。
- 各カラムには、以下の項目を記入します。
    - 第 1 カラムはアカウント名
    - 第 2 カラムはパスワード
    - 第 3 カラムはコメント、日本語も記述可能
    - 第 4 カラムはポリシー番号
- 一般的な表計算ソフトなどからのインポートでは、数字または記号などで始まるユーザ名、パスワード、コメントなどが含まれている場合、これらが数値、数式、日付と解釈され、正常に処理されない場合がありますので、ご注意ください。

● **手順 1：［インポート］画面を開く**

FEREC 管理ページより［設定］→［認証］→［内部認証］→［インポート］画面を開きます。

● **手順 2: ファイル名の設定**

直接、または、［参照］ボタンを押して、インポートするファイル名を設定します。

● **手順 3: インポート**

［インポート］ボタンを押すと、ファイル名を設定したファイルを FEREC にインポートします。

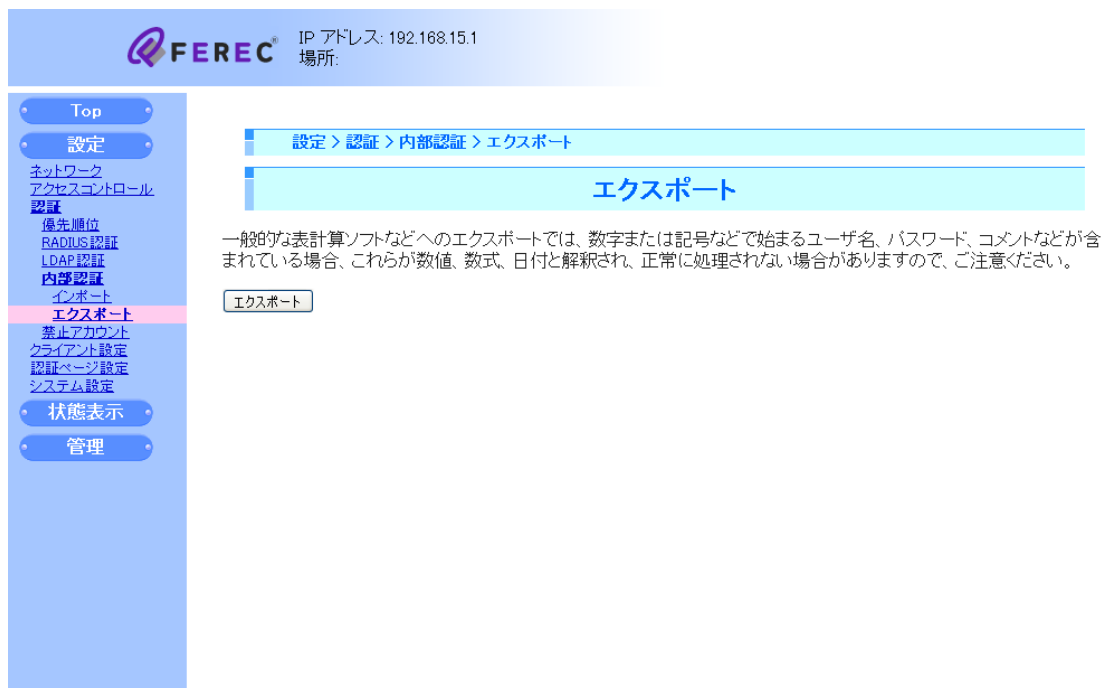
6.3.4.2. エクスポート

エクスポートでは、内部認証に登録済みのアカウントを管理用 PC に保存することができます。

NOTE

- 一般的な表計算ソフトなどへのエクスポートでは、数字または記号などで始まるユーザ名、パスワード、コメントなどが含まれている場合、これらが数値、数式、日付と解釈され、正常に処理されない場合がありますので、ご注意ください。

● **手順 1：［エクスポート］画面を開く**

FEREC 管理ページより［設定］→［認証］→［内部認証］→［エクスポート］画面を開きます。

● **手順 2: エクスポート**

［エクスポート］ボタンを押すと、内部認証に登録済みのアカウントを管理用 PC に保存できます。

6.3.5. 禁止アカウント

禁止アカウントでは、クライアント PC からの利用を禁止するアカウントを設定します。これにより、認証サーバの設定を変更することなく、特定のアカウントの利用を一時的に禁止することができます。

FEREC で禁止可能なアカウントは最大 20 件です。

工場出荷時に禁止しているアカウントはありません。

NOTE

- ログイン中のユーザを禁止アカウントに設定すると、直ちにログアウトされ、利用できなくなります。

禁止アカウントを追加する場合

- **手順 1：［禁止アカウント］画面を開く**

FEREC 管理ページより、［設定］→［認証］→［禁止アカウント］画面を開きます。

- **手順 2: 追加を始める**

  ［新しい禁止アカウントの追加］ボタンを押し、入力画面を開きます。

- **手順 3: アカウント名の設定**

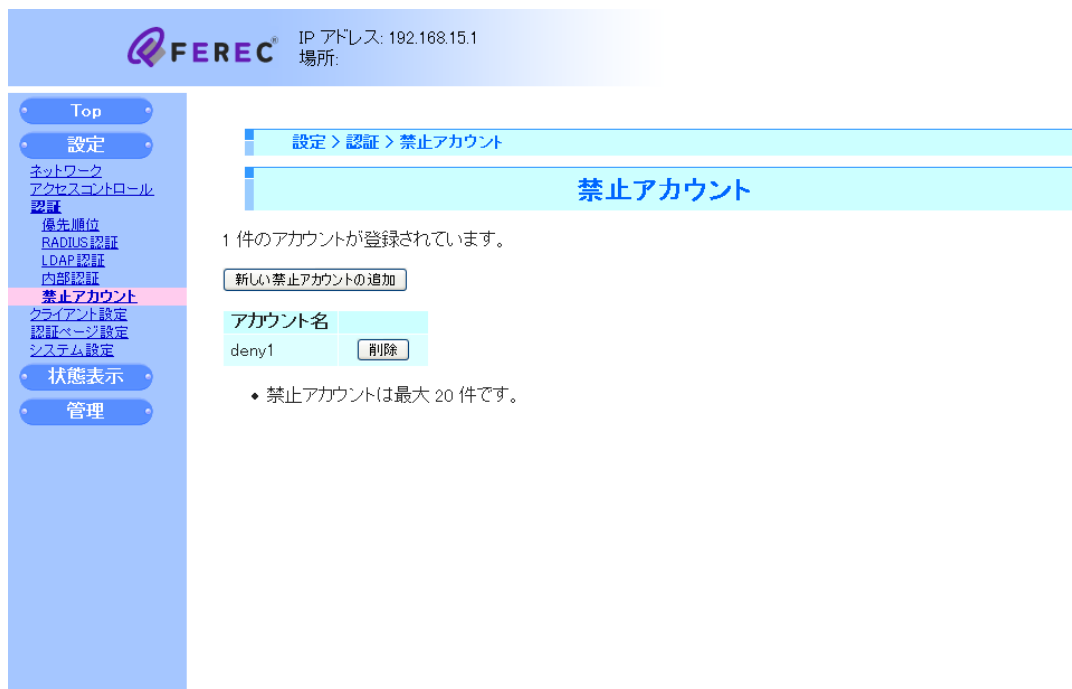
  ［アカウント名］欄に禁止するユーザアカウント名を設定します。アカウント名は半角 1 文字以上 31 文字以下で記入します。

- **手順 4: 設定**

  ［設定］ボタンを押すと禁止アカウントとして追加されます。追加されたアカウントは［禁止アカウント］画面上に一覧として表示され、削除が可能となります。

禁止アカウントを削除する場合

- 手順 1：［禁止アカウント］画面を開く

  FEREC 管理ページより、［設定］→［認証］→［禁止アカウント］画面を開きます。

- 手順 2: 削除する

  削除したいアカウントの［削除］ボタンを押すと、禁止アカウントから削除されます。

6.4. クライアント設定

［クライアント設定］のメニューには、以下の設定項目があります。

設定項目	概要
HTTP 外部プロキシ設定	プロキシ使用時に認証ページを強制表示するための設定を行います。
重複ログイン	同一ユーザによる複数 IP アドレスからのログインを許可するかどうかの設定を行います。
ポーリング間隔	クライアントをポーリングする間隔の設定を行います。
利用時間帯制限	ユーザの利用時間帯制限の設定を行います。

設定 > クライアント設定

クライアント設定

HTTP 外部プロキシ設定 プロキシ使用時に認証ページを強制表示するための設定を行います。
重複ログイン 同一ユーザによる複数 IP アドレスからのログインを許可するかどうかの設定を行います。
ポーリング間隔 クライアントをポーリングする間隔の設定を行います。
利用時間帯制限 ユーザの利用時間帯制限の設定を行います。

6.4.1. HTTP 外部プロキシ設定

HTTP 外部プロキシ設定では、クライアント PC で利用する HTTP プロキシサーバを設定します。

HTTP 外部プロキシ設定を行うと、クライアント PC において HTTP プロキシを使用した場合でも HTTP プロキシを使用しない場合と同様に、FEREC 認証ページを強制的に表示することができます。

NOTE

- 本機能は、クライアント PC の HTTP プロキシ設定を代替するものではありません。

HTTP 外部プロキシを使用する場合

- **手順 1：［HTTP 外部プロキシ設定］画面を開く**

FEREC 管理ページより、［設定］→［クライアント設定］→［HTTP 外部プロキシ設定］画面を開きます。

● **手順 2: プロキシサーバの編集画面を開く**

［編集］ボタンを押し、プロキシサーバの編集画面を開きます。

● **手順 3: プロキシサーバの設定**

使用する HTTP プロキシサーバの数に応じて、プロキシサーバ 1 からプロキシサーバ 5 までの IP アドレスとポート番号を設定します。IP アドレスは半角で記入します。ポート番号は 1～65535 の範囲から半角数字で記入します。いずれも前後に空白文字が入らないようにしてください。

● **手順 4: 設定**

［設定］ボタンを押すと、HTTP プロキシサーバを設定します。

● **手順 5: ［HTTP 外部プロキシ設定］画面に戻る**

［戻る］ボタンを押して、プロキシサーバの編集を終了し、［HTTP 外部プロキシ設定］画面に戻ります。

● **手順 6: 外部プロキシ設定の選択**

［外部プロキシ設定］プルダウンメニューから、「使用する」を選択します。

● **手順 7: 設定**

［設定］ボタンを押すと、HTTP 外部プロキシ設定が行われ、FEREC は自動的に再起動します。

HTTP 外部プロキシを使用しない場合

● **手順 1：［HTTP 外部プロキシ設定］画面を開く**

FEREC 管理ページより、［設定］→［クライアント設定］→［HTTP 外部プロキシ設定］画面を開きます。

● **手順 2: 外部プロキシ設定の選択**

［外部プロキシ設定］プルダウンメニューから、「使用しない」を選択します。

● **手順 3: 設定**

［設定］ボタンを押すと、HTTP 外部プロキシ設定が行われ、FEREC は自動的に再起動します。

HTTP プロキシサーバを変更する場合

- 手順 1：［HTTP 外部プロキシ設定］画面を開く

FEREC 管理ページより、［設定］→［クライアント設定］→［HTTP 外部プロキシ設定］画面を開きます。

● **手順 2: プロキシサーバの編集画面を開く**

［編集］ボタンを押し、プロキシサーバの編集画面を開きます。

● **手順 3: プロキシサーバの変更**

プロキシサーバ1からプロキシサーバ5までのIPアドレスとポート番号を変更します。いずれも前後に空白文字が入らないようにしてください。

● **手順 4: 設定**

［設定］ボタンを押すと、HTTP プロキシサーバを変更します。外部プロキシ設定が［使用する］に設定されている場合は、FEREC は自動的に再起動します。

6.4.2. 重複ログイン

重複ログインでは、複数の IP アドレスから同一のアカウントで重複してログインすることを許可できます。

工場出荷時、重複ログインは禁止しています。

NOTE

- 認証に RADIUS サーバを使用している場合、RADIUS サーバで Port-Limit 属性を追加することによって、重複ログインを許可した場合の同時ログイン数を制限することができます。

- **手順 1：［重複ログイン］画面を開く**

FEREC 管理ページより、［設定］→［クライアント設定］→［重複ログイン］画面を開きます。

- **手順 2: 重複ログイン設定の選択**

［重複ログイン］プルダウンメニューから、「禁止する」または「許可する」を選択します。

- **手順 3: 設定**

［設定］ボタンを押すと、重複ログインの設定が変更されます。

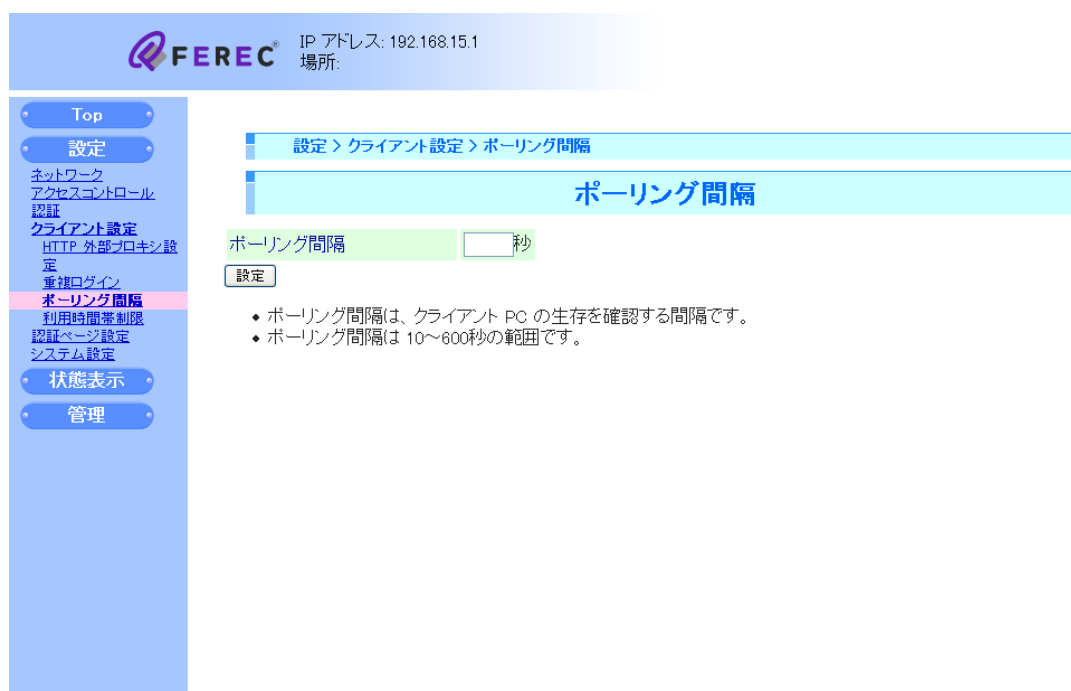
6.4.3. ポーリング間隔

ポーリング間隔では、クライアント PC の生存を確認する間隔を設定できます。

FEREC では、ポーリング間隔で設定された間隔でクライアント PC の生存を確認し、生存が確認できなかったクライアント PC は、ログアウトしたと見なします。なお、クライアント PC の生存は、ARP 要求をクライアント PC に送信し、応答があるかどうかで判定しています。

工場出荷時、ポーリング間隔は 120 秒に設定されています。

- **手順 1：［ポーリング間隔］画面を開く**

FEREC 管理ページより、［設定］→［クライアント設定］→［ポーリング間隔］画面を開きます。

- **手順 2: ポーリング間隔の設定**

［ポーリング間隔］欄にポーリング間隔を設定します。ポーリング間隔は 10～600 秒の範囲内で 1 秒単位に半角数字で入力します。前後に空白文字が入らないようにしてください。

- **手順 3: 設定**

［設定］ボタンを押すと、ポーリング間隔が指定した秒数に変更されます。

6.4.4. 利用時間帯制限

利用時間帯制限では、クライアント PC からの利用時間帯を制限させる設定を行います。

すべてのクライアント PC 共通で、利用可能な時間帯を 1 組、5 分単位で指定することができます。利用開始時刻の方が利用終了時刻より遅い場合は、利用可能な時間は翌日にかけた指定になります。なお、利用可能時間内に FEREC で認証を受けていても、利用可能時間を過ぎたら利用できなくなります。

工場出荷時、利用時間帯制限はありません。

利用時間帯を制限する場合

- **手順 1：［利用時間帯制限］画面を開く**

  FEREC 管理ページより、［設定］→［クライアント設定］→［利用時間帯制限］画面を開きます。

- **手順 2: 利用時間帯制限の選択**

  ［利用時間帯制限］のプルダウンメニューから「使用する」を選択します。

- **手順 3: 利用開始時刻の選択**

  ［利用開始時刻］のプルダウンメニューから開始時刻を選択します。

- **手順 4: 利用終了時刻の選択**

  ［利用終了時刻］のプルダウンメニューから終了時刻を選択します。

- **手順 5: 設定**

  ［設定］ボタンを押すと、利用時間帯が制限されます。

利用時間帯制限を解除する場合

- **手順 1：［利用時間帯制限］画面を開く**

  FEREC 管理ページより、［設定］→［クライアント設定］→［利用時間帯制限］画面を開きます。

- **手順 2: 利用時間帯制限の選択**

  ［利用時間帯制限］のプルダウンメニューから「使用しない」を選択します。

- **手順 3: 設定**

  ［設定］ボタンを押すと、利用時間帯の制限が解除されます。

6.5. 認証ページ設定

［認証ページ設定］のメニューには、以下の設定項目があります。

設定項目	概要
ロゴ表示	認証ページの FEREC ロゴの表示、非表示を設定します。
メッセージカタログ	認証ページに表示されるメッセージを編集します。
アクション設定	認証後のページの動作を指定することができます。

6.5.1. ロゴ表示

ロゴ表示では､クライアント PC の認証に表示される左フレームにある FEREC のロゴと FEREC のバージョンを非表示にできます。FEREC のバージョンや FEREC であることそれ自体をユーザに意識させたくない時には、非表示に変更してお使いください。

工場出荷時は、表示する設定になっています。

- **手順 1：［ロゴ表示］画面を開く**

FEREC 管理ページより、［設定］→［認証ページ設定］→［ロゴ表示］画面を開きます。

- **手順 2: ロゴ表示の選択**

［FEREC ロゴ］のプルダウンメニューから「表示しない」または「表示する」を選択します。

- **手順 3: 設定**

［設定］ボタンを押すと、ロゴ表示の設定が変更されます。

6.5.2. メッセージカタログ

メッセージカタログでは、クライアント PC の認証画面に表示するいくつかのメッセージを変更することができます。

変更可能なメッセージは、以下になります。

変更可能メッセージ一覧

識別子	既定メッセージ	説明
username	ユーザ名	認証画面のユーザ名入力フォームの名称を指定します。
password	パスワード	認証画面のパスワード入力フォームの名称を指定します。
login-button	ログイン	認証画面のログインボタンの名称を指定します。
logout-button	ログアウトする	ログアウト画面のログアウトボタンの名称を指定します。
auth-success	認証に成功しました。	認証に成功した時のメッセージを指定します。
client-unknown-ip	クライアント用 IP アドレスが不明です。	クライアントの IP アドレスが取得できなかった場合です。
client-out-of-service	利用時間外です。	利用時間帯制限によって利用を禁止されている時間帯です。
client-out-of-range	クライアント用アドレスの範囲外です。	クライアントの IP アドレスが FEREC の対象とするアドレス範囲外です。
already-login	ログイン中です。	ログインしているユーザが再度認証ページを表示した時のメッセージです。
logout-success	ログアウトに成功しました。3 秒後に認証ページに戻ります。	ログアウトに成功した時です。

（続く）

変更可能メッセージ一覧（続き）

識別子	既定メッセージ	説明
logout-failed	ログアウトに失敗しました。	ログアウトに失敗した時です。
auth-progress	認証しています...	認証サーバに問い合わせ中に表示するメッセージです。
auth-failed-already	{user} さんはすでにログインしています。(*1)	すでにログインしている同じ端末から同じユーザがログインを試みた場合です。エラーではありません。
auth-failed-multi	{user} さんはすでにログインしています。(*1)	重複ログインが禁止されていて、すでに他の端末などからログインしているユーザがログインを試みた場合です。
auth-failed-portlimit	{user} さんは同時ログインの最大数を超えました。(*1)	重複ログインが許可されていますが、その同時ログイン数を超えた場合です。
auth-failed-cred	認証に失敗しました。 ユーザ名かパスワードが違います。	ユーザ名かパスワードが違う場合です。
auth-failed-empty	ユーザ名が入力されていません。 ユーザ名を入力してください。	ユーザ名が入力されていない場合です。
auth-failed-timeout	認証に失敗しました。 認証サーバへの接続がタイムアウトしました。 管理者に連絡してください。	認証サーバへの接続がタイムアウトした場合です。
auth-failed-unreach	認証に失敗しました。 認証サーバに接続できません。 管理者に連絡してください。	RADIUS、LDAP 認証サーバに接続できなかった場合です。
auth-failed-protocol	認証に失敗しました。 認証プロトコルエラーです。 管理者に連絡してください。	認証サーバからの応答が正しく処理できなかった場合です。

（続く）

変更可能メッセージ一覧（続き）

識別子	既定メッセージ	説明
auth-failed-noauth	認証に失敗しました。 認証サーバが指定されていません。 管理者に連絡してください。	認証優先順位で認証サーバが指定されていない場合です。
auth-failed-reject	認証は拒否されました。 ログインは管理者により禁止されています。	禁止アカウントにより認証が禁止されている場合です。
auth-failed-full	ログインできません。 クライアント数の上限に達しています。	クライアント数の上限に達しているためログインできない場合です。
auth-failed-macaddr	認証に失敗しました。 MAC アドレスが登録されていません。	MAC アドレス認証を行っていて、MAC アドレスが登録されていないため認証に失敗した場合です。
auth-failed-internal	認証に失敗しました。 エラーが発生しました。 管理者に連絡してください。	その他のエラーです。

(*1) {user}は、ユーザ名に置き換えて表示されます。

メッセージを変更する場合

- 手順 1: ［メッセージカタログ］画面を開く

FEREC 管理ページより、［設定］→［認証ページ設定］→［メッセージカタログ］画面を開きます。

● **手順 2: 編集を始める**

変更するメッセージの右にある［編集］ボタンを押して、編集画面を開きます。

● **手順 3: ユーザ定義の選択**

［メッセージ］のラジオボタンから、「ユーザ定義」を選択します。

● **手順 4: メッセージの入力**

［ユーザ定義］欄にクライアント PC の認証画面に表示するメッセージを入力します。メッセージは半角 1 文字以上 200 文字（全角 100 文字相当）以下で記入します。

auth-failed-already、auth-failed-multi および auth-failed-portlimit のメッセージは、メッセージ中に“{user}”と記述すると、アカウント名に置き換えて表示されます。

● **手順 5: 設定**

［設定］ボタンを押すと、入力した内容にメッセージが変更されます。

メッセージを既定値に戻す場合

● 手順 1: ［メッセージカタログ］画面を開く

FEREC 管理ページより、［設定］→［認証ページ設定］→［メッセージカタログ］画面を開きます。

● **手順 2: 編集を始める**

変更するメッセージの右にある［編集］ボタンを押して、編集画面を開きます。

● **手順 3: 既定の選択**

メッセージのラジオボタンから、［既定］を選択します。

● **手順 4: 設定**

［設定］ボタンを押すと、メッセージが既定値に戻されます。

6.5.3. アクション設定

アクション設定では、クライアント PC の認証時、認証結果によってカスタムフレームに表示するページなどを設定できます。

アクション設定で表示するページを変更できるのは以下のケースです。

識別子	説明
success	認証に成功した時。 この時はクライアント情報を左フレーム(認証フレーム)に出力するかどうかについても設定ができます。
fail-passwd	ユーザ名かパスワードが原因で認証に失敗した時
fail-other	それ以外の原因で認証に失敗した時

表示するファイルは HTML エディタ等で作成して頂き、別途 “9. 認証ページカスタム領域へのアップロード” に従ってアップロードしてください。

認証に成功した時のアクションを変更する場合

- **手順 1: ［アクション設定］画面を開く**

  FEREC 管理ページより、［設定］→［認証ページ設定］→［アクション設定］画面を開きます。

● **手順 2: 編集を始める**

「認証に成功した時」の右にある［編集］ボタンを押して、編集画面を開きます。

● **手順 3: 動作の選択**

認証に成功した時に右フレームを変更しない場合は、［動作］のラジオボタンで「何もしない」を選択します。

認証に成功した時に右フレームをアップロードした任意のファイルに切り替えたい場合は、［動作］のラジオボタンで「右フレームを指定のファイルに変更」を選択し、そのファイル名を入力します。

ファイルはルートディレクトリにあるファイルのみ指定できます。ファイル名は半角の数字(ASCII コード 0x30～0x39)、英大文字(0x41～0x5a）、英小文字（0x61～0x7a)、ハイフン（0x2d)、ドット（0x2e）およびアンダースコア（0x5f）を使用して、126 文字以内で指定します。

- **手順 4: 左フレームにクライアント情報を出力する機能の設定**

認証に成功した時に、左(認証)フレームにユーザ名などのクライアント情報を出力することができます。ここで出力する情報は画面には表示されず、HTML の<INPUT type=hidden> タグとして出力されますので、右フレームで指定した任意のファイルから Javascript などのスクリプトで値を参照することができます。

まず［左フレームにクライアント情報を出力］のプルダウンメニューからこの機能を「使用する」か「使用しない」を選択します。

「使用しない」を選択した場合は個別のチェックボックスの状態に関わらず一切のクライアント情報を出力しません。

「使用する」を選択した場合は、さらに［出力する情報］欄の個別のチェックボックスで出力したい項目を指定します。ここでチェックを入れなかった項目は <INPUT> タグそのものを出力しません。チェックを入れた項目だけが左フレームに <INPUT type=hidden> タグとして出力されます。出力できる情報は以下の通りです。

識別子	説明
username	ログインしたユーザのユーザ名
policy-name	このクライアントに適用したポリシーの名前
policy-id	このクライアントに適用したポリシーの番号
mac-address	このクライアントの MAC アドレス(コロン区切り 16 進数形式)
hostname	FEREC の LAN 側ホスト名
wan-address	FEREC の WAN 側 IP アドレス(ドット区切り 10 進数形式)
location	FEREC の「場所名」
client-ip-address	このクライアントの IP アドレス(ドット区切り 10 進数形式)

- **手順 5: 設定**

［設定］ボタンを押すと、設定が変更されます。

NOTE

［左フレームにクライアント情報を出力］機能を使用する場合の、認証成功時の左フレームの HTML ソースには以下の書式で出力されます。

```
<INPUT type=hidden id="識別子" value="値">
```

例えばユーザ名が taro であればユーザ名の行は以下のようになります。

```
<INPUT type=hidden id="username" value="taro">
```

このクライアント情報は、右フレームからは Javascript で例えば以下のようにして値を取得することができます。

```
user = top.auth.document.getElementById("username").value;
// user に "taro" が代入されます
```

なお、Javascript は、ご利用の環境(OS、ウェブブラウザ、ウェブブラウザの設定等)によって動作しない場合がありますので、ご注意ください。

認証に失敗した時のアクションを変更する場合

- **手順 1: ［アクション設定］画面を開く**

FEREC 管理ページより、［設定］→［認証ページ設定］→［アクション設定］画面を開きます。

● **手順 2: 編集を始める**

「ユーザ名かパスワードが原因で認証に失敗した時」か「それ以外の原因で認証に失敗した時」の右にある［編集］ボタンを押して、編集画面を開きます。

● **手順 3: 動作の選択**

認証に失敗した時に右フレームを変更しない場合は、［動作］のラジオボタンで「何もしない」を選択します。

認証に失敗した時に右フレームをアップロードした任意のファイルに切り替えたい場合は、［動作］のラジオボタンで「右フレームを指定のファイルに変更」を選択し、そのファイル名を入力します。ファイル名の制約については前項「認証に成功した場合」を参照してください。

なお、認証に失敗した場合には、クライアント情報の出力は一切行いません。

● **手順 4: 設定**

［設定］ボタンを押すと、設定が変更されます。

6.6. システム設定

［システム設定］のメニューには、以下の設定項目があります。

設定項目	概要
管理許可アドレス設定	管理許可アドレスの設定を行います。
HTTPS 設定	HTTPS 接続の設定を行います。
RADIUS アカウンティング	RADIUS アカウンティングサーバの設定を行います。
syslog 設定	ログを転送する syslog サーバの設定を行います。
時刻設定	内部時計の設定、NTP サーバの設定を行います。
場所名設定	本体設置場所を記述します。
Center2 設定	Center2 についての設定を行います。

設定 > システム設定

システム設定

管理許可アドレス設定	管理許可アドレスの設定を行います。
HTTPS 設定	HTTPS 接続の設定を行います。
RADIUSアカウンティング	RADIUSアカウンティングサーバの設定を行います。
syslog設定	ログを転送する syslog サーバの設定を行います。
時刻設定	内部時計の設定、NTP サーバの設定を行います。
場所名設定	本体設置場所を記述します。
Center2 設定	Center2 についての設定を行います。

6.6.1. 管理許可アドレス設定

FEREC では、管理ページ、管理コンソール（telnet,ssh）およびカスタムページ用の FTP への接続を、許可した特定のアドレスからのみに制限することができます。

管理許可アドレス設定では、許可するアドレスを最大 5 個まで登録できます。

なお、MNT ポートにはこの管理許可アドレスによる制限は適用されず、常に接続できます。また、工場出荷時は制限していません。

管理許可アドレスを追加する場合

- **手順 1：［管理許可アドレス設定］画面を開く**

FEREC 管理ページより［設定］→［システム設定］→［管理許可アドレス設定］画面を開きます。

● **手順 2: アドレスの入力画面を開く**

［新しい管理許可アドレスの追加］ボタンを押して、アドレスの入力画面を開きます。

● **手順 3: 管理許可アドレスの入力**

［管理許可アドレス］欄に登録する IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。また、ネットマスク長をプルダウンメニューから選択します。管理許可アドレスはネットワークまたは単一ホストで指定します。ネットワーク全体を指定する場合は、192.168.45.0/24 のように CIDR 表記で指定します。単一のホストを指定する場合は、192.168.45.10/32 のようにネットマスク長を 32 にします。

● **手順 4: 設定**

［設定］ボタンを押すと管理許可アドレスが追加されます。

管理許可アドレスを削除する場合

- 手順 1： ［管理許可アドレス設定］画面を開く

　FEREC 管理ページより［設定］→［システム設定］→［管理許可アドレス設定］画面を開きます。

- 手順 2: 管理許可アドレスの削除

　管理許可アドレスの右横にある［削除］ボタンを押すと、該当のアドレスが管理許可アドレスから削除されます。

6.6.2. HTTPS 設定

HTTPS 設定では、クライアント PC の認証および管理ページへのアクセスに HTTP または HTTPS どちらを使用するか設定します。但し、クライアント PC の認証または管理ページへのアクセスどちらか一方を HTTP、もう一方を HTTPS のように別々の設定にすることはできません。

HTTPS を使用する場合は、先に"6.6.2.1. 証明書インポート"を行ってください。

なお、MNT ポートは、HTTPS 設定の設定内容にかかわらず、常に HTTP のみで接続できます。

- **手順 1：［HTTPS 設定］画面を開く**

FEREC 管理ページより［設定］→［システム設定］→［HTTPS 設定］画面を開きます。

- **手順 2: 接続プロトコルの選択**

［接続プロトコル］のプルダウンメニューから、使用するプロトコルとして「HTTP」または「HTTPS」どちらかを選択します。

- **手順 3: 設定**

［設定］ボタンを押すと、クライアント PC の認証および管理ページへのアクセスに使用するプロトコルが設定され、自動的に再起動します。

6.6.2.1. 証明書インポート

証明書インポートでは、HTTPS で使用する証明書及び鍵ファイルをインポートします。必要な場合は、中間 CA 証明書も使用できます。

各証明書および鍵ファイルは PEM 形式のみ使用できます。但し、パスフレーズの設定された鍵ファイルは使用できません。また、使用できる証明書および鍵ファイルはいずれも 16KB 以内です。

各証明書および鍵ファイルがすでにインポートしてある場合、再びインポートを行うと以前の証明書および鍵ファイルを上書きします。

- **手順 1: ［証明書インポート］画面を開く**

  FEREC 管理ページより［設定］→［システム設定］→［HTTPS 設定］→［証明書インポート］画面を開きます。

設定 > システム設定 > HTTPS 設定 > 証明書インポート

証明書インポート

サーバ証明書ファイル	参照...
鍵ファイル	参照...
中間CA証明書ファイル	参照...

インポート

- 各証明書、鍵は PEM 形式のみ使用できます。
- 各証明書と鍵がすでにインポートしてある場合、再びインポートを行うと以前の証明書と鍵を上書きします。
- パスフレーズの設定された鍵は使用できません。
- 証明書、鍵はいずれも 16KB 以内です。
- 中間 CA 証明書は必要のない場合省略することができます。

- **手順 2: サーバ証明書ファイル名の設定**

  ［サーバ証明書ファイル］欄に直接、または、［参照］ボタンを押して、サーバ証明書ファイルのファイル名を設定します。

- **手順 3: 鍵ファイル名の設定**

  ［鍵ファイル］欄に直接、または、［参照］ボタンを押して、鍵ファイルのファイル名を設定します。

- **手順 4: 中間 CA 証明書ファイル名の設定**

［中間 CA 証明書ファイル］欄に直接、または、［参照］ボタンを押して、中間 CA 証明書ファイルのファイル名を設定します。

中間 CA 証明書が不要な場合は、ファイル名を省略します。

- **手順 5: インポート**

［インポート］ボタンを押すと、ファイル名を設定した各ファイルを FEREC にインポートします。

6.6.2.2. 証明書エクスポート

証明書エクスポートでは、FEREC 本体にインポート済みの証明書ファイルを取り出すことができます。

- **手順 1：［証明書エクスポート］画面を開く**

  FEREC 管理ページより［設定］→［システム設定］→［HTTPS 設定］→［証明書エクスポート］画面を開きます。

- **手順 2: エクスポート**

  各ファイル名の右にある［エクスポート］ボタンを押すと、それぞれのファイルが管理用 PC に保存できます。

6.6.3. RADIUS アカウンティング

RADIUS アカウンティングでは、RADIUS アカウンティングに使用する RADIUS アカウンティングサーバを設定します。RADIUS アカウンティングサーバは、最大 2 台設定できます。なお、両方のサーバを設定した場合には、同じアカウンティング情報を両方のサーバに送信します。

RADIUS アカウンティングサーバを設定する場合

- 手順 1：［RADIUS アカウンティング］画面を開く

 FEREC 管理ページより、［設定］→［システム設定］→［RADIUS アカウンティング］画面を開きます。

● **手順 2: 編集を始める**

［RADIUS アカウンティングサーバ 1］または［RADIUS アカウンティングサーバ 2］にある［編集］ボタンを押します。

● **手順 3: サーバの設定**

［サーバ］欄に RADIUS アカウンティングサーバのホスト名または IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

● **手順 4: ポート番号の設定**

［ポート番号］欄に RADIUS アカウンティングサーバのポート番号を設定します。ポート番号は半角数字で記入します。前後に空白文字が入らないようにしてください。通常使用されるポート番号は 1813 か 1646 です。

● **手順 5: シークレットの設定**

［シークレット］欄に RADIUS アカウンティングサーバのシークレットを設定します。シークレットは 1 文字以上 127 文字以内の半角で記入します。

● **手順 6: タイムアウトの設定**

［タイムアウト］欄に RADIUS アカウンティングサーバへの接続とアカウンティング情報送信のタイムアウト値を設定します。タイムアウトは 1～60 秒の範囲から半角数字で記入します。前後に空白文字が入らないようにしてください。

● **手順 7: 設定**

［設定］ボタンを押すと、RADIUS アカウンティングサーバの設定が行われます。

RADIUS アカウンティングサーバを削除する場合

● **手順 1：［RADIUS アカウンティング］画面を開く**

FEREC 管理ページより、［設定］→［システム設定］→［RADIUS アカウンティング］画面を開きます。

● **手順 2: 削除する**

削除したいエントリの［削除］ボタンを押すと、削除されます。

6.6.4. syslog 設定

FEREC では、自身のログを外部の syslog サーバに送信することができます。syslog 設定では、syslog サーバを設定します。

- **手順 1：［syslog 設定］画面を開く**

  FEREC 管理ページより［設定］→［システム設定］→［syslog 設定］画面を開きます

- **手順 2: サーバ設定**

  ［サーバ名］欄に syslog サーバのホスト名または IP アドレスを設定します。前後に空白文字が入らないようにしてください。

- **手順 3: ファシリティの選択**

  ［ファシリティ］のプルダウンメニューから syslog サーバへログを送信する際のファシリティを選択します。選択可能なファシリティは、「local0」～「local7」です。

- **手順 4: レベルの選択**

  ［レベル］のプルダウンメニューから syslog サーバへ送信するレベルを選択します。

FEREC は、重大度がここで選択したレベル以上のログを syslog サーバへ送信します。重大度は高い方から順に、「ERR」、「WARN」、「NOTICE」、「INFO」、「DEBUG」となります。

なお、FEREC のユーザログは「NOTICE」以上、パケットログは「INFO」以上を設定すると syslog サーバへ送信されます。

- **手順 5: 設定**

  ［設定］ボタンを押すと syslog サーバが設定されます。

6.6.5. 時刻設定

時刻設定では、FEREC 本体の時刻を設定します。設定方法は、NTP サーバ指定か直接設定かを選ぶことができます。

NTP サーバを指定する場合

● **手順 1：［時刻設定］画面を開く**

FEREC 管理ページより［設定］→［システム設定］→［時刻設定］画面を開きます。

● **手順 2: NTP サーバの選択**

ラジオボタンで［NTP サーバ］を選択します。

● **手順 3: サーバの設定**

［NTP サーバ］欄に NTP サーバもしくは SNTP サーバのホスト名または IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

● **手順 4: 設定**

［設定］ボタンを押すと NTP サーバとの時刻同期を開始します。

時刻を直接設定する場合

- **手順 1：［時刻設定］画面を開く**

  FEREC 管理ページより［設定］→［システム設定］→［時刻設定］画面を開きます。

- **手順 2: 直接設定の選択**

  ［直接設定］の左にあるラジオボタンを選択します。

- **手順 3: 時刻の設定**

  「年」、「月」、「日」、「時」、「分」欄に時刻を設定します。いずれも前後に空白文字が入らないようにしてください。秒は 00 秒になります。

- **手順 4: 設定**

  ［設定］ボタンを押すと、指定した時刻に設定します。

6.6.6. 場所名設定

場所名設定では、設置場所等を識別するための名前を設定します。場所名は、FEREC 管理ページ上部に表示されます。

工場出荷時、場所名は設定されていません。

- **手順 1：［場所名設定］画面を開く**

  FEREC 管理ページより［設定］→［システム設定］→［場所名設定］画面を開きます。

- **手順 2: 場所名の設定**

  ［場所］欄に設置場所等を半角 63 文字(全角 31 文字)以内で設定します。

- **手順 3: 設定**

  ［設定］ボタンを押すと、場所名が設定されます。

6.6.7. Center2 設定

Center2 設定では、Center2 と連携するための設定を行います。

なお、Center2 と連携するには、Center2 においても FEREC を登録する必要があります。詳しくは「Center2 取扱説明書」をご覧ください。

- **手順 1：［Center2 設定］画面を開く**

FEREC 管理ページより［設定］→［システム設定］→［Center2 設定］画面を開きます。

- **手順 2: 場所名の設定**

［Center2 アドレス］欄に Center2 の IP アドレスを指定します。前後に空白文字が入らないようにしてください。

- **手順 3: 設定**

［設定］ボタンを押すと、Center2 が設定されます。

7. 状態表示

［状態表示］のメニューには、以下の機能があり、FEREC における各種状態を表示することができます。

機能	概要
ユーザ接続状況	ユーザの接続状況を一覧表示します。
DHCP 配布状況	DHCP サーバによるアドレスの割当状況を一覧表示します。
ログ	ログを表示します。
設定一覧	設定情報を一覧表示します。
本体情報	本体の情報を表示します。

状態表示

状態表示

ユーザ接続状況 ユーザの接続状況を一覧表示します。
DHCP配布状況 DHCP サーバによるアドレスの割当状況を一覧表示します。
ログ ログを表示します。
設定一覧 設定情報を一覧表示します。
本体情報 本体の情報を表示します。

7.1. ユーザ接続状況

ユーザ接続状況では、クライアント PC から FEREC への接続状況を確認することができます。

● **手順 1：［ユーザ接続状況］画面を開く**

FEREC 管理ページより［状態表示］→［ユーザ接続状況］画面を開くと、FEREC にログインしているユーザが表示されます。

なお、表示される項目は、以下のとおりです。

- IP アドレス
- ユーザ名
- MAC アドレス
- ポリシー名
- ログイン時刻

7.2. DHCP 配布状況

DHCP 配布状況では、DHCP によるクライアント PC への IP アドレス配布状況を確認することができます。

● **手順 1：［DHCP 配布状況］画面を開く**

FEREC 管理ページより［状態表示］→［DHCP 配布状況］画面を開くと、DHCP によるクライアント PC への IP アドレス配布状況が表示されます。

なお、表示される項目は、以下のとおりです。

- IP アドレス
- MAC アドレス
- リース開始
- リース終了
- ユーザ名

7.3. ログ

ログでは、FEREC 本体が出力する各種ログを確認することができます。

FEREC のログは、再起動時、初期化されます。また、一定量を超えた場合は、古いものから順に消されます。

そのため、ログの保存が必要な場合は、Center2 をご利用いただくか、または、syslog サーバを設定し、syslog サーバで保存してください。syslog サーバの設定は、“6.6.4. syslog 設定” を参照してください。

FEREC のログには、以下の 4 種類があります。

ログ種別	内容
システムログ	FEREC 本体に関するメッセージ
ユーザログ	ユーザの動向に関するメッセージ
パケットログ	アクセスコントロール(*)で採取したパケット情報
デバッグログ	保守に関するメッセージ

(*)アクセスコントロールについては、“6.2. アクセスコントロール”を参照してください。

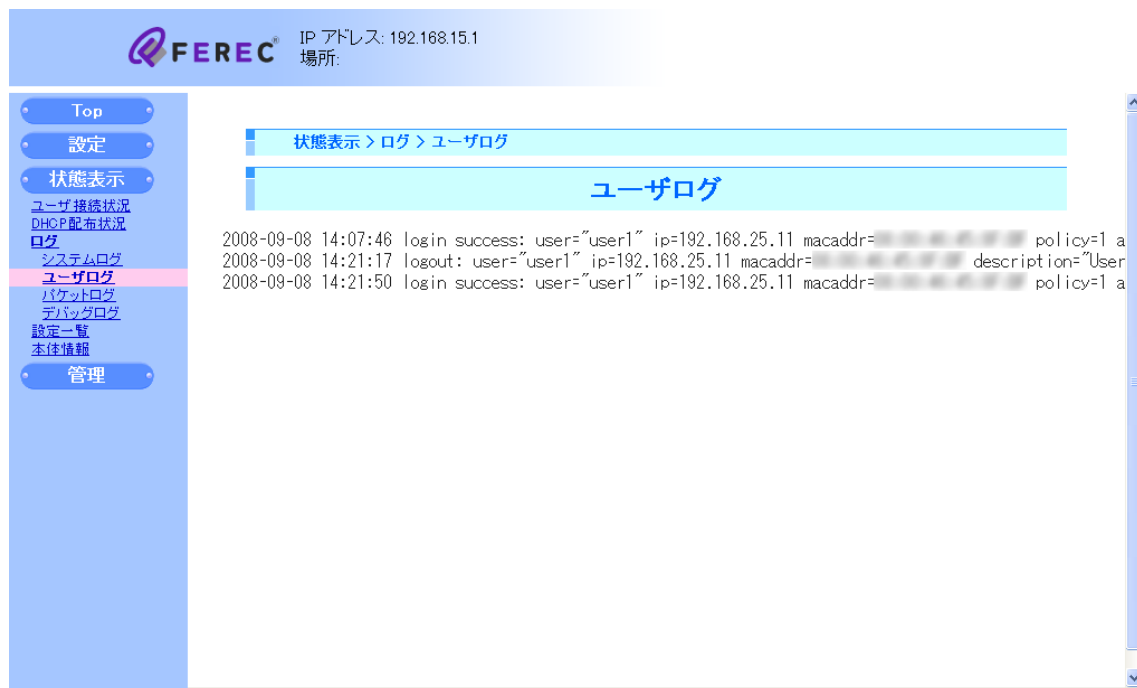
システムログを表示する場合

● **手順1：［システムログ］画面を開く**

FEREC 管理ページより［状態表示］→［ログ］→［システムログ］画面を開くと、システムログが古い順に表示されます。

ユーザログを表示する場合

- **手順１：［ユーザログ］画面を開く**

　FEREC 管理ページより［状態表示］→［ログ］→［ユーザログ］画面を開くと、ユーザログが古い順に表示されます。

パケットログを表示する場合

- **手順1：［パケットログ］画面を開く**

　FEREC 管理ページより［状態表示］→［ログ］→［パケットログ］画面を開くと、パケットログが古い順に表示されます。

デバッグログを表示する場合

- **手順1：［デバッグログ］画面を開く**

　FEREC 管理ページより［状態表示］→［ログ］→［デバッグログ］画面を開くと、デバッグログが古い順に表示されます。

7.4. 設定一覧

設定一覧では、FEREC 本体の設定内容を確認することができます。

- **手順 1：［設定一覧］画面を開く**

FEREC 管理ページより［状態表示］→［設定一覧］画面を開くと、現在動作中の設定内容が表示されます。

7.5.　本体情報

本体情報では、FEREC 本体の情報を確認することができます。

表示されるのは、以下の項目です。

- 品名
- 型番
- シリアル番号
- ファームウェアのバージョン
- WAN MAC アドレス
- LAN MAC アドレス
- MNT MAC アドレス

● **手順 1：［本体情報］画面を開く**

FEREC 管理ページより［状態表示］→［本体情報］画面を開くと、FEREC 本体の情報が表示されます。

8. 管理

［管理］のメニューには、以下の機能があります。

機能	概要
パスワード	管理者パスワードの設定を行います。
設定初期化	設定を初期化し、工場出荷時状態に戻します。
再起動	再起動を行います。
ステータスダンプ	障害解析用のステータスダンプを取得します。
バックアップ	設定のバックアップ、リストアを行います。
ファームウェア更新	ファームウェアの更新を行います。
ping	ping を使用して接続確認を行います。

パスワード　管理者パスワードの設定を行います。
設定初期化　設定を初期化し、工場出荷時状態に戻します。
再起動　再起動を行います。
ステータスダンプ　障害解析用のステータスダンプを取得します。
バックアップ　設定のバックアップ、リストアを行います。
ファームウェア更新　ファームウェアの更新を行います。
ping　ping を使用して接続確認を行います。

8.1. パスワード

パスワードでは､管理者パスワードおよび FTP パスワードを設定します｡管理者パスワードは、管理ページへのアクセスおよび管理コンソールへログインする際に、FTP パスワードは、カスタム領域用の FTP ログインに使用します。

管理者パスワードを設定する場合

● **手順 1：［パスワード］画面を開く**
FEREC 管理ページより［管理］→［パスワード］画面を開きます。

● **手順 2: パスワードの入力**
［管理者パスワード］欄に管理者パスワードを入力します。管理者パスワードは半角（ASCII コード 0x20～0x7e）3 文字以上 15 文字以下で記入します。

● **手順 3: 設定**
［管理者パスワード］欄下部の［設定］ボタンを押すと、直ちに管理者パスワードが変更されます。

FTP パスワードを設定する場合

- **手順 1：［パスワード］画面を開く**

 FEREC 管理ページより［管理］→［パスワード］画面を開きます。

- **手順 2: パスワードの入力**

 ［FTP パスワード］欄に FTP パスワードを入力します。FTP パスワードは半角（ASCII コード 0x20～0x7e）3 文字以上 15 文字以下で記入します。

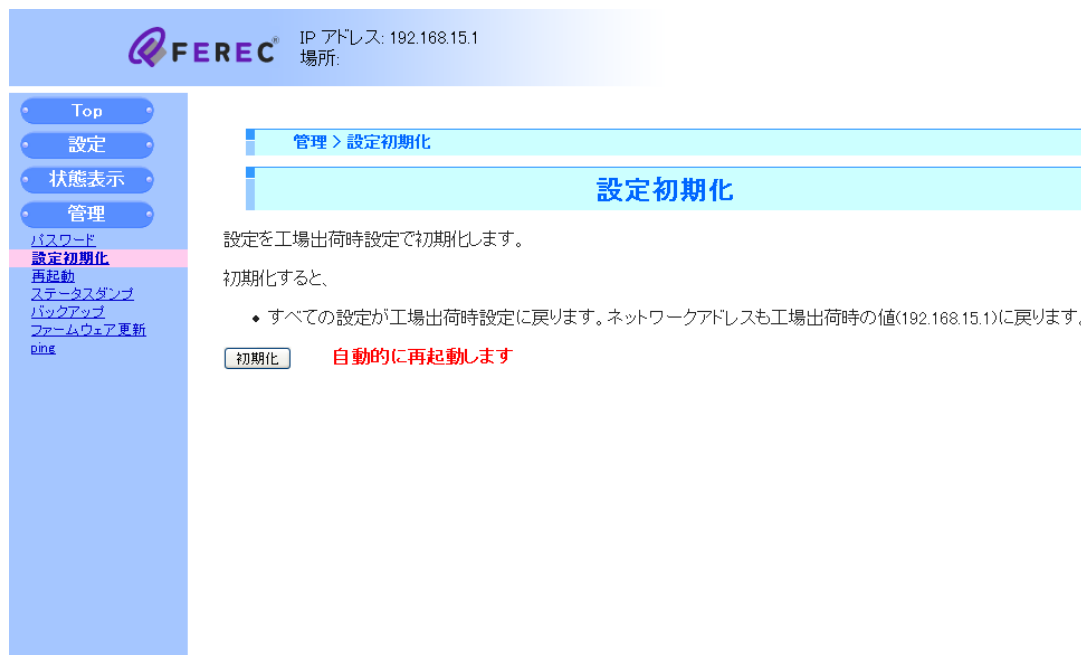
- **手順 3: 設定**

 ［FTP パスワード］欄下部の［設定］ボタンを押すと、直ちに FTP パスワードが変更されます。

8.2. 設定初期化

設定初期化では、FEREC の設定を初期化します。初期化すると、すべての設定が工場出荷時設定に戻ります。ネットワークアドレスも工場出荷時の値(192.168.15.1)に戻ります。

- **手順 1： ［設定初期化］画面を開く**

  FEREC 管理ページより［管理］→［設定初期化］画面を開きます。

- **手順 2: 初期化**

  ［初期化］ボタンを押すと、FEREC の設定が初期化され、自動的に再起動します。

8.3. 再起動

FEREC を再起動します。再起動すると、すべてのユーザは切断され、ログは初期化されます。

- **手順 1：［再起動］画面を開く**

  FEREC 管理ページより［管理］→［再起動］画面を開きます。

- **手順 2: 再起動**

  ［再起動］ボタンを押すと、FEREC が再起動します。

8.4. ステータスダンプ

ステータスダンプは、FEREC 内部の情報をダンプしたバイナリファイルです。FEREC に障害が発生した場合などに、ステータスダンプを弊社サポートセンターにご提供頂けますと、問題の早期解決につながることが期待できます。

NOTE

- ステータスダンプには、再起動すると消えてしまう情報も多く含まれておりますので、FEREC の動作に問題が発生した場合は、再起動を試される前にステータスダンプを保存しておかれることをお勧めします。

- **手順 1：［ステータスダンプ］画面を開く**

  FEREC 管理ページより［管理］→［ステータスダンプ］画面を開きます。

- **手順 2: ステータスダンプ保存**

  ［実行］ボタンを押すと、ステータスダンプを管理用 PC に保存します。

8.5. バックアップ

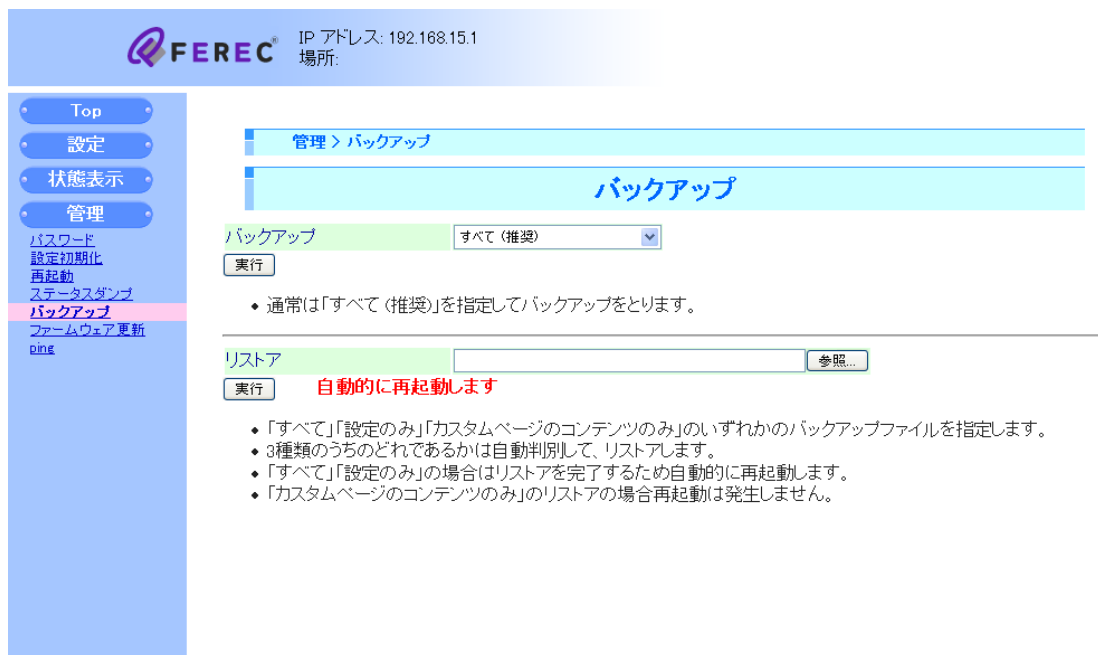
バックアップでは、FEREC の設定内容を管理用 PC に保存します。また、保存したバックアップファイルをリストアして、設定内容を復元できます。

NOTE

- バックアップファイルは、そのままリストアして下さい。例えば、一度解凍して再圧縮したような加工したバックアップファイルによるリストアは、動作保証しておりません。

バックアップする場合

- **手順 1：［バックアップ］画面を開く**

 FEREC 管理ページより［管理］→［バックアップ］画面を開きます。

- **手順 2: バックアップ対象の選択**

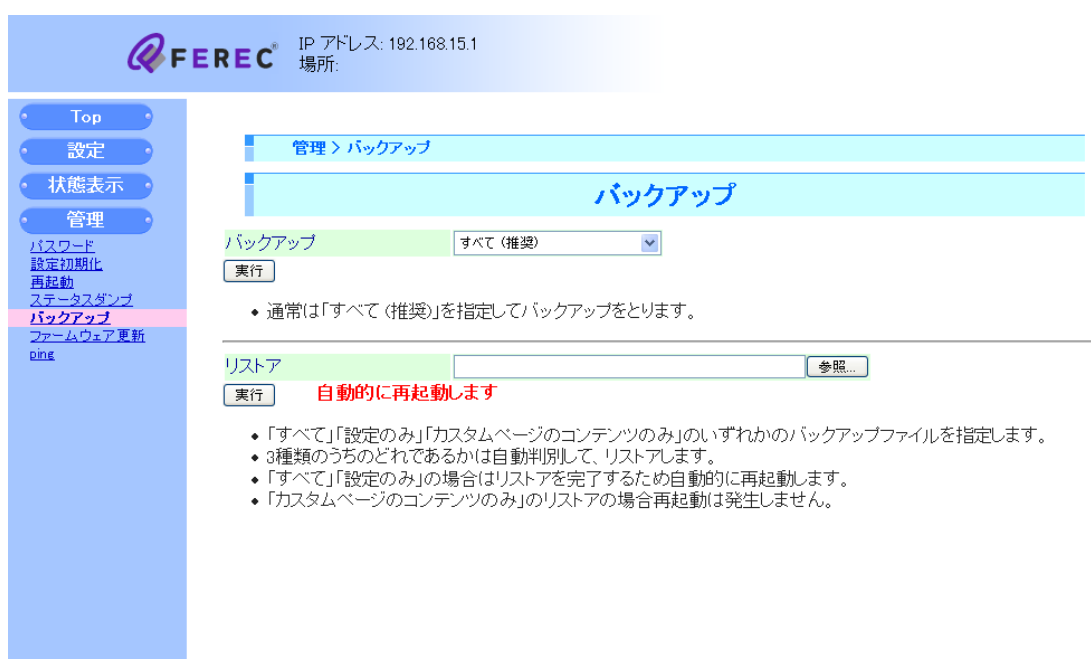
 ［バックアップ］プルダウンメニューでバックアップ対象を選択します。「すべて」、「設定のみ」または「カスタムページのコンテンツのみ」から選択できますが、通常は「すべて（推奨）」を選択してください。なお、リストア時には、バックアップファイルの種類は自動的に判別するため、特に指定する必要はありません。

● **手順 3: バックアップ実行**

［実行］ボタンを押すと、バックアップファイルを管理用 PC に保存することができます。

リストアする場合

● **手順 1: ［バックアップ］画面を開く**

FEREC 管理ページより［管理］→［バックアップ］画面を開きます。

● **手順 2: ファイル名の設定**

［リストア］欄に直接、または、［参照］ボタンを押して、バックアップファイルのファイル名を設定します。

● **手順 3: リストア実行**

［リストア］欄下部の［実行］ボタンを押すと、設定内容が復元され、FEREC は自動的に再起動します。但し、「カスタムページのコンテンツのみ」をリストアした場合は再起動しません。

8.6. ファームウェア更新

FEREC は、常に最新のファームウェアでご利用頂く事をお勧めします。

FEREC のファームウェアを更新することにより、ご購入後に新たに追加・改良された機能をご利用いただくことができます。

なお、ファームウェアの更新中には電源を切らないでください。

また、ファームウェアをダウングレードした場合は、設定およびカスタムページのコンテンツが初期化される事があります。

NOTE

- 以下の型番の FEREC は、それぞれ対応しているファームウェアのバージョンが違います。対応バージョンより、低いバージョンにダウングレードする事は出来ません。

型番	対応バージョン
FAJ521	2.2.3 以上
FAJ522	2.4.2 以上
FBJ721	2.2.1 以上
FBJ722	2.4.3 以上

- **手順 1：ファームウェアのダウンロード**

  FEREC のファームウェアを http://www.ferec.jp/ より管理用 PC にダウンロードしてください。

- **手順 2: クライアントのログアウト**

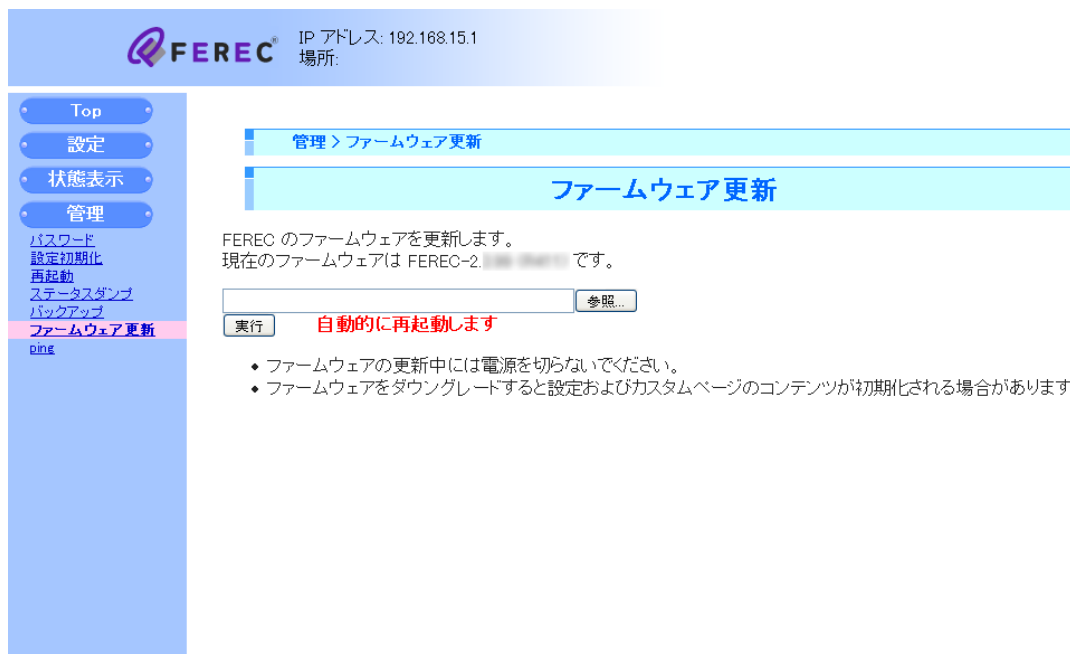
  すべてのクライアント PC がログアウトしていることを確認してください。ファームウェア更新後 FEREC は自動的に再起動しますので、その際ログインしているユーザはログアウトさせられます。

- **手順 3: 設定のバックアップ**

  ファームウェアの更新（アップグレード）では設定は保存されますが、万が一の状況に備え、必ず事前に設定のバックアップを取ってください。

  バックアップ方法については、“8.5. バックアップ”を参照して下さい。

● **手順 4: ［ファームウェア更新］画面を開く**

FEREC 管理ページより［管理］→［ファームウェア更新］画面を開きます。

● **手順 5: ファームウェアファイルの選択**

直接入力または、［参照］ボタンを押して、ダウンロードしておいたファームウェアファイルを選択します。

● **手順 6: ファームウェア更新**

［実行］ボタンを押すと、ファームウェアが更新され、FEREC は自動的に再起動します。

● **手順 7: ファームウェアバージョンの確認**

再起動が完了したら、再び FEREC 管理ページより［状態表示］→［本体情報］画面を開き、ファームウェアのバージョンで更新したバージョンであることを確認してください。

8.7. ping

ping では、FEREC から ping を行い、相手先との疎通を確認します。

- **手順 1: ［ping］画面を開く**

  FEREC 管理ページより［管理］→［ping］画面を開きます。

- **手順 2:ホスト名または IP アドレスの入力**

  ［ホスト名または IP アドレス］欄に、ホスト名または IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

- **手順 3: ping 実行**

  ［ping 実行］ボタンを押すと、ping を実行し、実行結果が表示されます。

NOTE

- ホスト名を使用する場合は、DNS サーバが設定されている必要があります。DNS サーバの設定方法は、“6.1.3. DNS 設定”を参照してください。

9. 認証ページカスタム領域へのアップロード

FEREC ユーザ認証画面の右フレームに、ウェブコンテンツを表示することが可能です。「お知らせ」、「連絡事項」などをアップロードして組織内ポータルサイトとしてご利用いただけます。

なお、表示するウェブコンテンツデータは、FTP を使用してアップロードします。

9.1. MNT ポートに接続する場合

① PC の LAN ポートと FEREC の MNT ポートをクロス結線の LAN ケーブルで直接接続します。

② PC のネットワーク設定は DHCP クライアントとして設定を行います。

③ PC は DHCP サーバからの IP アドレス割り当てに失敗し、自動的に PC には 169.254.***.***という IP アドレスが割り当てられます。この際、IP アドレスが割り当てられるまで約 1 分程度かかります。

④ PC で FTP クライアントソフトを起動し、169.254.35.1 に接続します。ユーザ名は webadmin、パスワードは設定してある FTP パスワードを入力します。工場出荷時のパスワードは webadmin です。

NOTE

- もしパスワードが不明になった場合は、FEREC 管理ページ、もしくは FEREC 管理コンソールからパスワードを変更することが可能です。

9.2. WAN または LAN ポート経由で接続する場合

9.2.1. FEREC がブリッジモードで動作している場合

① PC と FEREC をネットワークを経由して接続します。もし PC と FEREC を直接 LAN ケーブルで接続する場合は、PC の LAN ポートと FEREC の WAN ポートまたは LAN ポートをクロス結線の LAN ケーブルで接続します。

② PC はネットワーク環境に応じてネットワーク設定を行います。

③ PC で FTP クライアントソフトを起動し、FEREC の IP アドレスに接続します。ユーザ名は webadmin、パスワードは設定してある FTP パスワードを入力します。工場出荷時のパスワードは webadmin です。

9.2.2. FEREC が NAT/NAPT モードで動作している場合

① PC と FEREC をネットワークを経由して接続します。もし PC と FEREC を直接 LAN ケーブルで接続する場合は、PC の LAN ポートと FEREC の WAN ポートまたは LAN ポートをクロス結線の LAN ケーブルで接続します。

② PC はネットワーク環境に応じてネットワーク設定を行います。

③ FEREC の WAN 側ネットワークから接続する場合は、PC で FTP クライアントソフトを起動し、FEREC の WAN 側 IP アドレスに接続します。または、FEREC の LAN 側ネットワークから接続する場合は、PC で FTP クライアントソフトを起動し、FEREC の LAN 側 IP アドレスに接続します。ユーザ名は webadmin、パスワードは設定してある FTP パスワードを入力します。工場出荷時のパスワードは webadmin です。

NOTE

- 工場出荷時の FEREC はブリッジモードで動作しており、FEREC の IP アドレスは、192.168.15.1 です。PC と FEREC を直接 LAN ケーブルで接続する場合、ブリッジモードでは、DHCP サーバ機能は動作しませんので、PC のネットワーク設定で 192.168.15.2 などの IP アドレスを設定しておく必要があります。

- FEREC の設定で、管理ページへのアクセス制限を行っている場合は、許可された IP アドレスからのみ FTP 接続することができます。管理ページへのアクセス制限については、“6.6.1. 管理許可アドレス設定”を参照して下さい。

9.3. コンテンツアップロード時の注意事項

FEREC 認証ページへコンテンツをアップロードする際には以下の点に注意してください。

- 接続時のフォルダ（ディレクトリ）がドキュメントルートとなります。トップページのファイル名は index.html としてアップロードしてください。
- 使用するフォルダ名、ファイル名は半角英数文字を使用してください。
- アップロード可能なデータ容量は約 4MB です。容量制限により FTP クライアントでエラーが発生した場合は、不要なファイルを FTP クライアントの削除機能で消去するなどして、ご利用ください。
- CGI は動作しません。
- コンテンツの中で、FEREC の WAN(外部)側ネットワーク上へのリンクを張った場合、認証通過前はリンク先の表示はできません。必要な場合は、アクセスコントロールの anonymous ポリシーのルールであらかじめ該当リンク先ウェブサーバへの通信を許可しておいてください。

10. CLI コマンド

10.1. CLI コマンド一覧

FEREC の CLI で使用可能なコマンドは以下になります。

CLI コマンド一覧

コマンド	頁
account radius1 delete	173
account radius1 server *server*:*port* *secret* *timeout*	172
account radius2 delete	173
account radius2 server *server*:*port* *secret* *timeout*	172
admin center2 add *address*	174
admin center2 delete	174
admin https { enable | disable }	174
admin network add *address*/*mask*	173
admin network delete *address*/*mask*	173
admin sshd { enable | disable }	173
admin telnetd { enable | disable }	173
auth guest add *username* *password* *comment* *policy-id*	172
auth guest delete *username*	172
auth ldap1 basedn *basedn*	171
auth ldap1 binddn *binddn* *bindpw*	171
auth ldap1 bindtype { direct | indirect }	171
auth ldap1 delete	172
auth ldap1 login-attribute *attribute*	171
auth ldap1 policy-attribute *attribute*	171
auth ldap1 server *uri* *policy-id* *timeout*	170
auth ldap1 version { 2 | 3 }	172
auth ldap2 basedn *basedn*	171
auth ldap2 binddn *binddn* *bindpw*	171
auth ldap2 bindtype { direct | indirect }	171
auth ldap2 delete	172

（続く）

CLI コマンド一覧（続き）

コマンド	頁
auth ldap2 login-attribute *attribute*	171
auth ldap2 policy-attribute *attribute*	171
auth ldap2 server *uri* *policy-id* *timeout*	170
auth ldap2 version { 2 | 3 }	172
auth order *auth1* [*auth2* [*auth3* [*auth4* [*auth5*]]]]	169
auth radius1 delete	170
auth radius1 server *server*:*port* *secret* *policy-id* *timeout*	169
auth radius1 with-macaddr delete	170
auth radius1 with-macaddr password *password*	170
auth radius2 delete	170
auth radius2 server *server*:*port* *secret* *policy-id* *timeout*	169
auth radius2 with-macaddr delete	170
auth radius2 with-macaddr password *password*	170
auth reject add *username*	172
auth reject delete *username*	172
client multiple-login { enable | disable }	174
client polling-interval *seconds*	174
client schedule { enable | disable }	174
client schedule open *hh*:*mm* *HH*:*MM*	174
debug auth { enable | disable }	182
debug dhcp { enable | disable }	182
dhcp { enable | disable }	169
dhcp lease-time *minutes*	169
dhcp pool *address* *num*	169
exit	182
html action *action-id* contents *filename*	175
html action *action-id* none	175
html action attach { enable | disable }	175
html action attach *actkey* { enable | disable }	176
html logo { enable | disable }	175
html message *msgkey* *message*	175
html message *msgkey* default	175

（続く）

CLI コマンド一覧（続き）

コマンド	頁
`http-proxy { enable	disable }`	180
`http-proxy server add` *address*:*port*	180
`http-proxy server delete` *address*:*port*	180
`https-cert delete all`	181
`initialize`	182
`logout`	182
`network default-route add` *address*	168
`network default-route delete`	168
`network dns1 add` *address*	168
`network dns1 delete`	169
`network dns2 add` *address*	168
`network dns2 delete`	169
`network lan-address` *address*/*mask*	167
`network lan-hostname` *hostname*	168
`network nat-mapping` *wan-address lan-address num*	168
`network type { bridge	nat	napt }`	167
`network wan-address` *address*/*mask*	167
`ntp { enable	disable }`	176
`ntp server add` *server*	177
`ntp server delete`	177
`password admin` *password*	173
`password webadmin` *password*	173
`ping` *host*	182
`policy add` *policy-id name*	177
`policy delete` *policy-id*	177
`policy ftp-proxy { enable	disable }`	179
`policy rule add` *policy-id rule-id act dir proto address*/*mask* [*port*]	178
`policy rule delete` *policy-id rule-id*	178
`restart`	182
`set date` *yyyy-mm-dd HH*:*MM*	181
`set location` *location*	182

（続く）

CLI コマンド一覧（続き）

10.2. CLI コマンド説明

FEREC の CLI で使用可能なコマンドの一覧を示します。
なお、各コマンドの機能については、“6. 設定” から “8. 管理” もあわせてご覧下さい。

各コマンドについては、以下のように表記しています。

show config
タイプライターで示した文字はコマンドであることを示します。
val
イタリックで示した文字は変数であることを示します。
{ A | B | C | … }
A、B、C、… のいずれかのうち 1 つを示します。
[*val* **]**
val が省略可能であることを示します。

コマンドで指定する文字列が、空白や記号を含む場合は"（ダブルクォート）で文字列全体をクォートしてください。

network type { bridge | nat | napt }
ネットワークの動作タイプを決定します。bridge、nat、napt はそれぞれブリッジモード、NAT モード、NAPT モードを示します。
設定は再起動後に有効になります。

network wan-address ***address/mask***
FEREC 本体のアドレスおよびネットマスクを CIDR 表記で指定します。NAT または NAPT モードの場合は WAN 側のアドレスおよびネットマスクの意味になります。
設定は再起動後に有効になります。

network lan-address ***address/mask***
FEREC 本体の LAN 側アドレスおよびネットマスクを CIDR 表記で指定します。NAT または NAPT モードの時のみ意味を持ちます。
設定は再起動後に有効になります。

network nat-mapping ***wan-address lan-address num***

NAT または NAPT モードの時のクライアントの範囲や 1:1 NAT のアドレスを指定します。

NAPT モードなら *lan-address* から *num* 個の連続した IP アドレスを FEREC のクライアント用アドレスとします。*wan-address* の値は NAPT モードでは使用しません。

NAT モードなら *lan-address* に対応する WAN 側のアドレスを *wan-address* で指定します。以後 *num* 個の連続した IP アドレスを 1:1 NAT 用に使用します。

設定は再起動後に有効になります。

network lan-hostname ***hostname***

FEREC の LAN 側ホスト名を FQDN で指定します。LAN 側ホスト名は、主にクライアントから見える FEREC の FQDN で、次の 2 つの用途に用います。

ユーザ認証ページ URL として用います。空文字列の場合 URL は IP アドレス表記になります。また、ドメイン部は、NAT または NAPT モードでクライアントに配布する DHCP の Domain オプションの値になります。

設定は再起動後に有効になります。

network default-route add ***address***

デフォルトゲートウェイを指定します。

設定は再起動後に有効になります。

network default-route delete

デフォルトゲートウェイの指定を削除します。

設定は再起動後に有効になります。

network dns1 add ***address***

network dns2 add ***address***

DNS サーバを指定します。DNS サーバは FEREC 本体のホスト名の逆引き等に使用します。NAT または NAPT モードではクライアントに対して FEREC が DNS サーバになりますが、その際の上流 DNS サーバになります。なお、DNS サーバは、最大 2 台まで設定できます。

設定は即有効になります。

network dns1 delete
network dns2 delete

DNS サーバの設定を削除します。
設定は即有効になります。

dhcp { enable | disable }

NAT または NAPT モードの場合に FEREC の DHCP サーバを起動するかどうかを指定します。初期状態では enable です。
LAN 側のクライアントの IP アドレスをすべて固定的に割り振ってあるなどの理由で DHCP サーバが不要の場合は disable にすることができます。
ブリッジモードの場合、この設定は無効です。DHCP サーバは起動しません。
設定は再起動後に有効になります。

dhcp pool *address num*

NAT または NAPT モードの場合に DHCP サーバがアドレスを配る範囲を指定します。
指定は network nat-mapping コマンドで指定した *lan-address* から *num* 個の範囲内で、*address* から連続する *num* 個の 1 区間のみ指定できます。
NAT または NAPT モードで DHCP が有効であれば、変更は即有効になります。

dhcp lease-time *minutes*

NAT または NAPT モードの場合に DHCP サーバがアドレスを配るリースのリース時間を分単位で指定します。初期値は 60 分で、1 分～1440 分の範囲で指定可能です。
NAT または NAPT モードで DHCP が有効であれば、変更は即有効になります。

auth order *auth1* [*auth2* [*auth3* [*auth4* [*auth5*]]]]

認証優先順位を決定します。*auth1*～*auth5* は認証サーバを指定します。認証サーバは、guest、radius1、radius2、ldap1、ldap2 から指定します。
認証サーバは 1 つ以上 5 つまで記述できます。
但し、サーバが設定されていない RADIUS、LDAP サーバは、認証優先順位を設定していても認証時無視します。
設定は即有効になります。

auth radius1 server *server*:*port secret policy-id timeout*
auth radius2 server *server*:*port secret policy-id timeout*

認証サーバ（RADIUS サーバ）を指定します。RADIUS サーバの設定は 2 セット持つことができるため auth radius1 または auth radius2 で指定します。

server は RADIUS サーバのホスト名もしくは IP アドレスを指定します。

port はポート番号を指定します。標準のポート番号を使用する場合でも *port* を省略することはできません。

secret は RADIUS サーバの共有シークレットを、*policy-id* はこの認証サーバの既定ポリシー番号を、*timeout* はタイムアウト値を秒単位で指定します。

auth radius1 with-macaddr password *password*

auth radius2 with-macaddr password *password*

RADIUS サーバ 1 もしくは RADIUS サーバ 2 でクライアントの MAC アドレス認証を行うようにし、その際に使用するパスワードを設定します。パスワードは、1 文字以上 127 文字以下で指定します。

設定は即有効になります。

auth radius1 with-macaddr delete

auth radius2 with-macaddr delete

RADIUS サーバ 1 もしくは RADIUS サーバ 2 でクライアントの MAC アドレス認証を行わないようにし、MAC アドレス認証用のパスワードを削除します。

auth radius1 delete

auth radius2 delete

RADIUS サーバ 1 もしくは RADIUS サーバ 2 の設定を削除します。

auth ldap1 server *uri policy-id timeout*

auth ldap2 server *uri policy-id timeout*

認証サーバ（LDAP サーバ）の指定をします。LDAP サーバ設定は 2 セット持つことができるため `auth ldap1` または `auth ldap2` で指定します。

uri は *proto*://*server* [:*port*]/という書式で、*proto* は `ldap` もしくは `ldaps`、*server* にはホスト名か IP アドレスを指定します。*port* はポート番号で省略可能です。省略した場合は標準ポート（LDAP なら 389、LDAPS なら 636）となります。

policy-id はこの認証サーバの既定ポリシー番号を、*timeout* はタイムアウト値を秒単位で指定します。

設定は即有効になります。

auth ldap1 bindtype { direct | indirect }
auth ldap2 bindtype { direct | indirect }

LDAP サーバのバインド方法を選択します。

indirect は間接バインドであり、指定のバインド DN で一旦バインドした後、ベース DN 以下を検索する方式です。direct は直接バインドであり、ベース DN 直下の DN に直接バインドする方式です。通常は indirect（間接バインド）を使用します。

設定は即有効になります。

auth ldap1 binddn *binddn bindpw*
auth ldap2 binddn *binddn bindpw*

LDAP サーバのバインド DN とバインドパスワードを指定します。

この設定は、間接バインド方式の時のみ有効で、直接バインド時には無効です。

設定は即有効になります。

auth ldap1 basedn *basedn*
auth ldap2 basedn *basedn*

LDAP サーバの検索ベース DN を指定します。

間接バインド方式の場合、指定した検索ベース DN 以下を検索します。一方、直接バインド方式の場合、指定した検索ベース DN の直下を login-attribute=*ユーザ名, basedn* という DN でバインドします。

設定は即有効になります。

auth ldap1 login-attribute *attribute*
auth ldap2 login-attribute *attribute*

LDAP サーバのユーザを検索する際の属性を指定します。

設定は即有効になります。

auth ldap1 policy-attribute *attribute*
auth ldap2 policy-attribute *attribute*

LDAP サーバのバインドした DN から、FEREC のアクセスポリシー名として取得する属性を指定します。

省略した場合はユーザごとのポリシー指定は行われず、このサーバの既定ポリシーが適用されます。また指定の属性名がエントリに存在しない、あるいは取得した値と同名のポリシー名が FEREC に存在しない場合も既定ポリシーが適用されます。

設定は即有効になります。

auth ldap1 version { 2 | 3 }

auth ldap2 version { 2 | 3 }

LDAP サーバの LDAP プロトコルのバージョンを指定します。

初期状態ではバージョン 2 です。

設定は即有効になります。

auth ldap1 delete

auth ldap2 delete

LDAP サーバ 1 もしくは LDAP サーバ 2 のすべての情報を削除します。

auth reject add *username*

禁止アカウントの追加を行います。

追加は即有効になります。

auth reject delete *username*

禁止アカウントの削除を行います。

削除は即有効になります。

auth guest add *username password comment policy-id*

内部認証アカウントの追加を行います。

username は追加するアカウント名を、*password* はパスワードを、*comment* はコメントを、*policy-id* はポリシー番号を指定します。

ユーザ名、パスワード、コメントはいずれも 31 バイト以内で指定します。

auth guest delete *username*

内部認証アカウントの削除を行います。

このアカウント名で既にログイン中のユーザは影響を受けません。

account radius1 server *server*:*port secret timeout*

account radius2 server *server*:*port secret timeout*

RADIUS アカウンティングサーバを指定します。

RADIUS アカウンティングサーバの設定は 2 セット持つことができるため、`account radius1` または `account radius2` で指定します。

server は RADIUS アカウンティングサーバのホスト名もしくは IP アドレスを、*port* はポート番号を指定します。標準のポート番号を使用する場合でも *port* を省略することはできません。

secret は RADIUS アカウンティングサーバの共有シークレットを、*timeout* はタイムアウト値を秒単位で指定します。

account radius1 delete
account radius2 delete

RADIUS アカウンティングサーバ 1 もしくは RADIUS アカウンティングサーバ 2 の設定を削除します。

password webadmin *password*

カスタムページ用の FTP パスワードを設定します。初期値は webadmin です。
設定は即有効になります。

password admin *password*

管理ページ GUI および CLI へのログインパスワードを設定します。初期値は admin です。なお、ログインアカウント名は admin 固定です。
設定は即有効になります。

admin network add *address/mask*

管理ページへ接続できるネットワークまたはホストを CIDR 表記で指定します。アクセス制限は 5 つまで記述できます。何も記述しない場合はすべての接続を許可します。デフォルトはすべての接続を許可です。
アクセス制限は管理ページ、telnet や ssh による CLI、FTP 接続に適用されます。MNT ポートからの接続にアクセス制限を適用することはできません。
設定は即有効になります。

admin network delete *address/mask*

管理ページへ接続を許可しているネットワークまたはホストを削除します。
設定は即有効になります。

admin sshd { enable | disable }

CLI への ssh でのログインを許可するかどうかを指定します。
この設定に関わらず MNT ポートからは常に telnet でのみログイン可能です。

admin telnetd { enable | disable }

CLI への telnet でのログインを許可するかどうかを指定します。
この設定に関わらず MNT ポートからは常に telnet でのみログイン可能です。

admin https { enable | disable }

管理ページおよびユーザ認証ページに HTTPS を使用するかどうかを指定します。enable なら HTTPS を、disable なら HTTP を使用します。デフォルトは disable です。

設定は再起動後に有効になります。

なお MNT ポートの管理ページはこの設定の影響を受けず常に HTTP です。

HTTPS を使用するには、先にサーバ証明書、秘密鍵（必要な場合は中間 CA 証明書も）をインポートしておく必要があります。但し、サーバ証明書、秘密鍵および中間 CA 証明書は CLI では設定できませんので、WebUI からインポートしてください。

admin center2 add *address*

この FEREC を管理する Center2 を指定します。*address* は Center2 の IP アドレスを指定します。ホスト名で指定することはできません。

設定は即有効になります。

admin center2 delete

Center2 の指定を削除します。

設定は即有効になります。

client polling-interval *seconds*

クライアントの生存を確認するポーリング間隔を指定します。*seconds* は秒数を指定します。デフォルトは 120 秒です。

client multiple-login { enable | disable }

重複ログインを許可するかどうかを指定します。enable で許可、disable で禁止します。

client schedule { enable | disable }

利用時間帯制限機能を利用するかどうかを指定します。

client schedule open *hh*:*mm* *HH*:*MM*

利用時間帯制限機能でユーザが FEREC を利用できる時間帯を指定します。

24 時間表記で毎日 *hh:mm* から *HH:MM* まで利用できることを示します。*hh:mm* よりも *HH:MM* のほうが小さい場合は *hh:mm* から日をまたいで翌日の *HH:MM* まで利用可能であることを示します。

この設定は利用時間帯制限機能が利用可能である時のみ有効になります。

html logo { enable | disable }

ユーザ認証ページの認証フレーム中にある FEREC のロゴとバージョンを表示するかどうかを指定します。enable で表示、disable で非表示にします。

html message *msgkey* default

html message *msgkey* *message*

ユーザ認証ページの認証フレーム中のメッセージを変更します。

msgkey はメッセージの識別子、*message* はメッセージを指定します。*message* の代わりに default を指定するとメッセージを初期状態に戻します。

変更可能なメッセージについては、“6.5.2. メッセージカタログ”を参照して下さい。

html action *action-id* none

html action *action-id* contents *filename*

ユーザ認証ページで、認証結果ごとの認証ページの動作を指定します。

action-id は識別子で以下のいずれかを指定します。

action-id	説明
success	認証に成功した時
fail-passwd	ユーザ名かパスワードが原因で認証に失敗した時
fail-other	それ以外の原因で認証に失敗した時

動作が none なら何もアクションを起こしません。また動作が contents ならカスタムページ(右側のフレーム)を *filename* で指定されたページに変更します。*filename* はカスタムページ用領域のトップディレクトリにあるファイルのみ指定することができます。サブディレクトリにあるファイルや別のサーバにあるファイル(URL)を指定することは出来ません。

html action attach { enable | disable }

認証成功時の左フレームにクライアント情報を出力するかどうかを指定します。disable なら出力しません。enable なら以下のコマンドで出力するパラメータを個別に指定します。

html action attach *actkey* { enable | disable }

認証成功時の左フレームに出力するクライアント情報を個別に指定します。この指定は html action attach enable である場合のみ意味を持ちます。*actkey* は識別子で以下のいずれかを指定します。

actkey	説明
username	ログインしたユーザのユーザ名
policy-name	このクライアントに適用したポリシーの名前
policy-id	このクライアントに適用したポリシーの番号
mac-address	このクライアントの MAC アドレス(コロン区切り 16 進数形式)
hostname	FEREC の LAN 側ホスト名
wan-address	FEREC の WAN 側 IP アドレス(ドット区切り 10 進数形式)
location	FEREC の「場所名」
client-ip-address	このクライアントの IP アドレス(ドット区切り 10 進数形式)

syslog facility *facility* *level*

syslog サーバへ送信するファシリティとレベルを指定します。

facility は local0～local7 の中から指定します。*level* は err、warn、notice、info、debug の中から指定し、指定したレベルとそれより重要度の高いログだけを送信します。設定は syslog server add コマンドで syslog サーバが指定されていれば、即有効になります。

syslog server add *server*

syslog サーバをホスト名か IP アドレスで指定します。

指定できる syslog サーバは 1 つだけです。syslog はこのコマンドで syslog サーバが指定されている場合のみ送信されます。

設定は即有効になります。

syslog server delete

syslog サーバの指定を削除します。

設定は即有効になります。

ntp { enable | disable }

FEREC の時刻を SNTP を用いて SNTP サーバもしくは NTP サーバに同期するかどうかを指定します。enable なら SNTP を用いて同期を行い、disable なら同期を行いません。FEREC はいずれの場合も NTP サーバにはなりません。

設定は即有効になります。

ntp server add ***server***

FEREC が参照する SNTP サーバもしくは NTP サーバをホスト名もしくは IP アドレスで指定します。

指定できるサーバは 1 つだけです。

設定は即有効になります。

ntp server delete

NTP サーバの指定を削除します。

設定は即有効になります。

policy add ***policy-id name***

ポリシー番号 *policy-id* のポリシーを追加します。ポリシー名は *name* で指定します。すでにポリシーが存在していれば名前の更新となります。

policy delete ***policy-id***

ポリシー番号 *policy-id* のポリシーを削除します。RADIUS および LDAP サーバの既定ポリシー、内部認証アカウント、スタティック NAT、スタティックブリッジのいずれかから参照しているポリシーは削除することができません。またポリシー0 およびポリシー1 を削除することは出来ません(内容を編集することはできます)。

`policy rule add` ***policy-id rule-id act dir proto address/mask*** **[*port*]**

ポリシー番号 *policy-id* のルール番号 *rule-id* のポリシールールを定義します。ポリシー *policy-id* は `policy add` コマンドにより定義されている必要があります。またルール *rule-id* がすでに定義されている場合はルールの上書きになります。

act は動作で以下のいずれかを指定します。

act	説明
`pass`	パケットの通過を許可します。
`drop`	パケットの通過を禁止します。TCP に対しては TCP RST を返し、UDP, ICMP には ICMP Unreach を返します。
`pass-log`	`pass` と同じですが、同時にパケットログに出力します。
`drop-log`	`drop` と同じですが、同時にパケットログに出力します。

dir はルールの方向で以下のいずれかを指定します。

dir	説明
`in`	WAN 側から LAN 側方向
`out`	LAN 側から WAN 側方向

proto はプロトコル名もしくはプロトコル番号です。

proto	説明
`all`	すべてのプロトコル
`tcp`	TCP（6）
`udp`	UDP（17）
`gre`	GRE（47）

これ以外のプロトコルは数値（1～255）で指定します。但し IPv4 上のプロトコルでなければ制御できません。

address/mask はターゲットとなるアドレス範囲で、IP アドレスもしくは IP アドレスとネットマスクを CIDR 形式で指定します。0.0.0.0/0 は `any` と記述することもできます。*port* はポート番号範囲の指定で、*proto* が TCP か UDP の場合のみ有効です。*port* は単一のポート番号か、ポート番号の範囲指定が行えます。範囲指定の場合 “21-23” のように空白を入れずにハイフンで繋げて指定します。

`policy rule delete` ***policy-id rule-id***

ポリシー番号 *policy-id* のルール番号 *rule-id* のポリシールールを削除します。

policy ftp-proxy { enable | disable }

アクセスコントロールの FTP プロキシ機能を有効にするかどうか指定します。

enable の場合アクセスコントロールで TCP/21 を許可すると、FTP の制御セッションをプロキシしデータコネクションが通過できるように内部のフィルタの制御を自動的に行います。但しブリッジや NAT モードであっても FTP の制御セッションだけはクライアントの(WAN 側)アドレスからではなく FEREC 本体から張られることになります。これが問題になる環境では disable にしてください。一切 FTP プロキシを行わなくなります。

static-nat add *wan-address lan-address mac-address policy-id comment*

スタティック NAT を追加します。

wan-address は WAN 側の IP アドレスを、*lan-address* は LAN 側の IP アドレスを、*policy-id* はこのスタティック NAT に適用するポリシー番号を、*comment* はコメントを指定します。

mac-address はこのスタティック NAT の LAN 側機器の MAC アドレスを限定したい場合に指定します。MAC アドレスを限定しない場合は、any を指定してください。

ブリッジモードで起動している間は設定を更新するだけでチェックは行われず、有効にもなりません。

static-nat delete *wan-address*

WAN 側アドレスが *wan-address* で示されるスタティック NAT を削除します。

ブリッジモードで起動している間は設定を更新するだけでチェックは行われず、有効にもなりません。

static-bridge add *wan-address mac-address policy-id comment*

スタティックブリッジを設定します。

wan-address はスタティックブリッジの IP アドレスを、*policy_id* はこのスタティックブリッジに適用するポリシー番号を、*comment* はコメントを指定します。

mac-address はこのスタティックブリッジの LAN 側機器の MAC アドレスを限定したい場合に指定します。MAC アドレスを限定しない場合は any を指定してください。

NAT または NAPT モードで起動している間は設定を更新するだけでチェックは行われず、有効にもなりません。

static-bridge delete *wan-address*

IP アドレスが *wan-address* で示されるスタティックブリッジを削除します。

NAT または NAPT モードで起動している間は設定を更新するだけでチェックは行われず、有効にもなりません。

static-route add *dst-address/mask gw-address comment*

スタティックルートを設定します。

dst-address/mask はデスティネーションアドレスとネットマスク長を CIDR 表記で、*gw-address* はゲートウェイアドレスを、*comment* はコメントを指定します。

ブリッジモードで起動している間は設定を更新するだけでチェックは行われず、有効にもなりません。

static-route delete *dst-address/mask*

デスティネーションアドレスが *dst-address/mask* であるスタティックルートを削除します。

ブリッジモードで起動している間は設定を更新するだけでチェックは行われず、有効にもなりません。

http-proxy { enable | disable }

HTTP 外部プロキシ機能を有効にするかどうかを指定します。

設定は再起動後に有効になります。

http-proxy server add *address:port*

HTTP 外部プロキシ機能のためのプロキシサーバを指定します。*address:port* はプロキシサーバの IP アドレスとポート番号を指定します。プロキシサーバは５つまで指定できます。

設定は再起動後に有効になります。

http-proxy server delete *address:port*

プロキシサーバの設定を削除します。*address:port* は削除するプロキシサーバの IP アドレスとポート番号を指定します。

設定は再起動後に有効になります。

show config

現在動作中の設定を表示します。

show config startup

次回起動時の設定を表示します。

show cpu

CPU の負荷状況とメモリの使用率を表示します。

show interface

ネットワークインタフェースの情報を表示します。

show arp

ARP テーブルを表示します。

show route

ルーティングテーブルを表示します。

show dhcp

DHCP のアドレス配布状況を表示します。

show client

ログインしているクライアントの一覧を表示します。

show log { user | system | packet | debug }

FEREC の揮発性メモリに保存されているログを表示します。
ログは古いものから順に削除されますので、Center2 をあわせてご利用いただくか、または、syslog サーバ等へ保存されることをお勧めします。
user はユーザログ、system はシステムログ、packet はパケットログ、debug はデバッグログです。

show version

FEREC 本体に関する情報を表示します。

show https-cert

サーバ証明書、秘密鍵および中間 CA 証明書がインポートされているかどうかを表示します。
インポートされていれば証明書の Subject,Issuer,有効期間を表示します。

https-cert delete all

HTTPS で使用するためにインポートした証明書及び鍵ファイルを FEREC から削除します。

set date *yyyy-mm-dd HH:MM*

時刻を設定します。秒は 00 秒になります。

set prompt *prompt*

CLI のプロンプトを *prompt* に設定します。15 文字以内です。デフォルトは空です。

set location *location*

FEREC の設置場所等を記述します。記述した内容は管理ページの上部に表示されます。記述した内容を削除するには *location* に””を指定します。

ping *host*

ping を実行します。*host* はホスト名もしくは IP アドレスで指定します。

debug auth { enable | disable }

`enable` にすると認証に関する詳細なデバッグ情報をデバッグログに出力します。デフォルトは `disable` です。

debug dhcp { enable | disable }

`enable` にすると NAT または NAPT 時の DHCP サーバに関する詳細なデバッグ情報をデバッグログに出力します。デフォルトは `disable` です。

restart

FEREC を再起動します。

initialize

FEREC を工場出荷時の状態に初期化し、再起動します。

logout

CLI からログアウトします。

exit

CLI からログアウトします。

11. ログ書式

FEREC で出力するユーザログおよびパケットログの書式について説明します。

NOTE

- なおこの書式は将来のバージョンで予告なく変更する場合があります。

11.1. ユーザログ書式

FEREC 管理ページから［状態表示］→［ログ］→［ユーザログ］画面で表示できるユーザログの書式について説明します。

11.1.1.ログイン成功

FEREC のユーザ認証に成功してログインした場合、出力するログは以下の書式になります。

```
login success: user="username" ip=ip-address macaddr=mac-address
policy=policy-id auth_serv=authserv
```

username はユーザ名、*ip-address* はクライアント PC の IP アドレスです。NAT または NAPT モードであれば LAN 側 IP アドレスを示します。
mac-address はクライアント PC の MAC アドレス、*policy-id* はこのユーザに適用したポリシー番号です。
authserv はこのユーザを認証した認証サーバを示しており、以下の 5 つのうちいずれかになります。

authserv	説明
guest	内部認証
radius1	RADIUS サーバ 1
radius2	RADIUS サーバ 2
ldap1	LDAP サーバ 1
ldap2	LDAP サーバ 2

11.1.2.ログイン失敗

FEREC のユーザ認証に失敗するなどしてログインできなかった場合には以下のようなログを出力します。

```
login failure: user="username" ip=ip-address macaddr=mac-address
auth_serv=authserv description="description"
```

username、*ip-address*、*mac-address*、*authserv* については認証成功時と同様です。*description* には認証に失敗した理由が示されます。
表示される *description* とその解説を以下に示します。

description	説明
Username is not specified	ユーザ名が空です。ユーザ名を入力してください。
Multi-login denied	すでに他の IP アドレスでログインしています。重複ログインが禁止のため、ログインできません。
Entry is full	同時にログインできるユーザ数を超過しており、ログインできません。
Login inhibited	禁止アカウントに登録されているため、ログインできません。
Authentication failed	認証に失敗しました。ユーザ名かパスワードが違う、あるいはサーバの設定を誤っている可能性があります。
Authentication server unreachable	RADIUS サーバに到達あるいは LDAP サーバに接続できませんでした。
Authentication server timeout	RADIUS 認証あるいは LDAP 認証でタイムアウトが発生しました。
Protocol error	（RADIUS 認証）サーバからの応答パケットのフォーマットが不正で処理できません。
MAC address authentication failed	MAC アドレスが違うために（RADIUS）認証に失敗しました。

11.1.3.ログアウト

FEREC からログアウトした場合に出力されるログは以下の書式になります。

```
logout: user="username" ip=ip-address macaddr=mac-address
description="description"
```

username はユーザ名、*ip-address* はクライアント PC の IP アドレスです。NAT または NAPT モードであれば LAN 側 IP アドレスを示します。

mac-address はクライアント PC の MAC アドレスです。

description はログアウトになった原因を示しており以下のいずれかになります。

description	説明
User Logout	ユーザが自主的にログアウトボタンを押したため。
No Response	クライアント PC から応答がなくなったため。
DHCP Released	DHCP リースが解放されたため。
System Rebooted	管理ページあるいは管理コンソールより再起動が行われたため。
Marked as inhibited user	禁止アカウントに追加されたため。
System service closed	利用時間帯制限を設定していて、利用終了時刻を過ぎたため。

11.2. パケットログ書式

FEREC 管理ページから［状態表示］→［ログ］→［パケットログ］画面で表示できるパケットログの書式について説明します。

ノーマルパケットの場合は、以下の書式になります。

date `policy` *policy-id*:`rule` *rule-id*:*type*:*proto* *src-ipaddress*(*src-user*):*src-port* > *dst-ipaddress*(*dst-user*):*dst-port*

date は日時、*policy-id* はポリシー番号、*rule-id* はルール番号です。*type* は許可(`pass`)か禁止(`drop`)を、*proto* はプロトコル種別です。

src-ipaddress は送信元 IP アドレス、*src-port* は送信元ポート番号、*dst-ipaddress* は送信先 IP アドレス、*dst-port* は送信先ポート番号です。

src-user は、FEREC の LAN 側から WAN 側への通信で、FEREC にログインしているユーザと送信元 IP アドレスが結びつく場合にユーザ名が表示されます。一方、*dst-user* は、FEREC の WAN 側から LAN 側への通信で、FEREC にログインしているユーザと送信先 IP アドレスが結びつく場合にユーザ名が表示されます。

フラグメントパケットの場合は、以下の書式になります。

date `policy` *policy-id*:`rule` *rule-id*:*type*:*proto* *src-ipaddress*(*src-user*):*src-port* > *dst-ipaddress*(*dst-user*):*dst-port* `fragment(id:`*id*, `offset:`*offset*)

id はフラグメントパケットの ID、*offset* は、フラグメントオフセットです。*date*、*policy-id*、*rule-id*、*type*、*proto*、*src-ipaddress*、*src-user*、*src-port*、*dst-ipaddress*、*dst-user* および *dst-port* は、ノーマルパケットの場合と同じです。

なお、2 個目以降のフラグメントパケットでは、*src-port* および *dst-port* は表示されません。

12. ハードウェア仕様

品名	FEREC520		
型番	FAJ520	FAJ521	FAJ522
外形寸法 (WxHxD)	214 x 30 x 151 mm	225 x 30 x 152 mm	210 x 33 x 150 mm
	（AC アダプタおよび突起部含まず）		
重量	0.9kg	1.2kg	1.0kg
	（AC アダプタ含まず）		
電源	AC100V 50/60Hz		
動作環境	温度: 10℃ ～ 40℃ 湿度: 10% ～ 90%（結露しないこと）		

品名	FEREC720		
型番	FBJ720	FBJ721	FBJ722
外形寸法 (WxHxD)	427 x 44 x 388 mm	440 x 44 x 325 mm	435 x 44 x 400 mm
	（突起部含まず）		
重量	5.8kg	5.0kg	6.2kg
電源	AC100V 50/60Hz		
動作環境	温度: 10℃ ～ 40℃ 湿度: 10% ～ 90%（結露しないこと）		

13. 保証とアフターサービス

お客様に安心してご使用頂くために

FEREC520 / FEREC720 の製品保証といたしまして、弊社工場出荷日より保証書に記載の期限までの無償保守サービスをご提供いたしております。

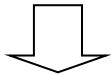
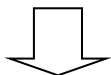
万一、保証期間中（保証書に明記されている期間)、製品の故障が発生した場合、下記のネットスプリング サポートセンターにご連絡下さい。

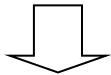
サポートセンターにて、お客様より症状をヒアリング及び診断後、代替機を速やかに発送いたします。

保証書(別添付)

保証書の規定に従って保守サービスを実施いたします。
記載内容をお確かめの上、大切に保管してください。

製品が故障したら・・

①サポートセンターにご連絡ください。

②サポートセンターで診断後、必要な場合、代替機（あるいは交換パーツ）を送付します。

③代替機が到着したら、お客様にて故障機と交換してください。

- 設定データの保証及び復旧などは行っておりません。お客様ご自身で予めバックアップ済みの設定データからリストアを行ってください。

④故障機をサポートセンターへご返送ください。

- 送料はお客様にてご負担をお願いいたします。
- 代替機交換後、ご返送頂いた製品は返却いたしません。
- お客様側で製品に貼られたシールなどは予めお剥がしの上ご返送ください。
- 製品の標準添付品以外は一切の保護をいたしませんので、予めご了承ください。

お問い合わせの前にご準備ください。

ユーザ登録がお済みでない場合、FERECホームページからユーザ登録を行ってください。製品のシリアル番号をご確認ください（シリアル番号が不明な場合は、サポートを受けることはできません）。

障害内容をできるだけ詳細にご説明頂けるようご準備ください。

保証書のご提示をお願いする場合がございます。

保証期間を過ぎているときは・・・

修理によって機能が維持できる場合は、お客様のご要望により有償で修理させて頂きます。

お問い合わせ窓口／機器送付先

FERECに関するお問い合わせは、下記サポートセンターまでお願いいたします。

〒108-0073 東京都港区三田3-12-16 山光ビル2階
（株）ネットスプリング サポートセンター

TEL：050-5536-4841
URL：http://www.ferec.jp/
E-MAIL：nssc@netspring.co.jp

受付対応時間　9:00～17:00（祝祭日および年末年始12/29～1/3を除く月～金）